فصلنامه پژوهش در مدیریت شماره ۴- دوره ۱- صفحات ۶۴۰-۶۲۷
Journal of Research in Management
Issn: 3060-6241

توسعه چارچوب امنیت اطلاعات برای زیرساخت‌های الکترونیکی شهرداری با تأکید بر تهدیدات سایبری نوظهور

علی حاجیانی [۱]، امیر اعتباری [۲]
۱ -کارشناسی فناوری اطلاعات، دانشگاه علمی کاربردی بوشهر. (رییس اداره زیرساخت و مرکز داده سازمان فناوری اطلاعات شهرداری بندر بوشهر)
۲- کارشناسی نرم افزار کامپیوتر، دانشگاه آزاد واحد دیلم. (رییس اداره فنی و پشتیبانی سازمان فناوری اطلاعات شهرداری بندر بوشهر)

چکیده

تحول دیجیتال و گسترش زیرساخت‌های الکترونیکی در شهرداری‌ها، زمینه‌ساز افزایش کارایی، شفافیت و کیفیت خدمات شهری شده است، اما هم‌زمان وابستگی روزافزون به سامانه‌های اطلاعاتی، شهرداری‌ها را در معرض تهدیدات سایبری پیچیده و نوظهور قرار داده است. داده‌های حساس شهروندی، سامانه‌های مالی، زیرساخت‌های حیاتی شهری و پلتفرم‌های شهر هوشمند، همگی اهداف جذابی برای مهاجمان سایبری محسوب می‌شوند و هرگونه اختلال یا نفوذ در آن‌ها می‌تواند پیامدهای عملیاتی، مالی و اجتماعی گسترده‌ای به همراه داشته باشد. در این شرایط، فقدان یک چارچوب جامع، یکپارچه و بومی‌سازی‌شده امنیت اطلاعات، یکی از مهم‌ترین چالش‌های مدیریت شهری دیجیتال در ایران به شمار می‌رود. هدف اصلی این پژوهش، توسعه یک چارچوب جامع امنیت اطلاعات برای زیرساخت‌های الکترونیکی شهرداری‌ها با تأکید بر شناسایی و مقابله با تهدیدات سایبری نوظهور است؛ چارچوبی که ضمن انطباق با استانداردهای بین‌المللی، با شرایط فنی، سازمانی و مدیریتی شهرداری‌های ایران سازگار باشد. روش تحقیق این مقاله از نوع مروری ـ تحلیلی است و با بهره‌گیری از مطالعات کتابخانه‌ای، بررسی اسناد و استانداردهای معتبر جهانی در حوزه امنیت اطلاعات و تحلیل پژوهش‌های داخلی مرتبط با شهرداری الکترونیک و شهر هوشمند انجام شده است. همچنین، زیرساخت‌های دیجیتال شهرداری‌ها، تهدیدات سایبری نوظهور و آسیب‌پذیری‌های فنی و مدیریتی آن‌ها به‌صورت نظام‌مند مورد بررسی قرار گرفته‌اند. یافته‌های پژوهش نشان می‌دهد که رویکردهای امنیتی فعلی در بسیاری از شهرداری‌ها پراکنده، واکنشی و فاقد انسجام راهبردی هستند و تمرکز بیش از حد بر ابزارهای فنی، بدون توجه به حکمرانی، مدیریت ریسک و تاب‌آوری سایبری، اثربخشی اقدامات امنیتی را کاهش داده است. بر این اساس، چارچوبی پنج‌ستونی شامل حکمرانی امنیت اطلاعات، شناسایی و ارزیابی ریسک، حفاظت فعال، تشخیص و واکنش سریع و بازیابی و تداوم خدمات ارائه شده است .

واژگان کلیدی: چارچوب امنیت اطلاعات، حکمرانی شهری دیجیتال، تهدیدات سایبری نوظهور، زیرساخت‌های الکترونیکی، مدیریت ریسک سایبری.

۱. مقدمه

تحول دیجیتال در بخش عمومی، به‌ویژه در سطح شهرداری‌ها، یک روند جهانی انکارناپذیر است که هدف آن بهینه‌سازی فرآیندهای مدیریتی، افزایش تعامل با شهروندان و ارائه خدمات عمومی با کیفیت‌تر و کارآمدتر است. این تحول، که اغلب ذیل مفهوم «شهر هوشمند» یا «حکمرانی دیجیتال شهری» تعریف می‌شود، زیرساخت‌های فناوری اطلاعات و ارتباطات (ICT) را به ستون فقرات عملیات روزمره تبدیل کرده است. از سامانه‌های مدیریت هوشمند ترافیک و حمل‌ونقل گرفته تا سامانه‌های شهروندی، مالیات، صدور پروانه و مدیریت پسماند، همگی بر بستر داده‌ها و زیرساخت‌های الکترونیکی عمل می‌کنند. این وابستگی فزاینده، اگرچه مزایای چشمگیری از منظر کارایی و دسترسی‌پذیری به همراه دارد، اما سازمان‌های شهری را در معرض طیف گسترده‌ای از ریسک‌های امنیتی قرار داده است که پیش‌تر در ساختارهای سنتی کمتر مورد توجه قرار می‌گرفتند. اهمیت این موضوع زمانی دوچندان می‌شود که ملاحظه کنیم داده‌های شهری، شامل اطلاعات هویتی شهروندان، داده‌های جغرافیایی حساس و اطلاعات حیاتی زیرساخت‌ها، از جمله اهداف اصلی مهاجمان سایبری محسوب می‌شوند (مرادزاده و همکاران، ۲۰۲۲).

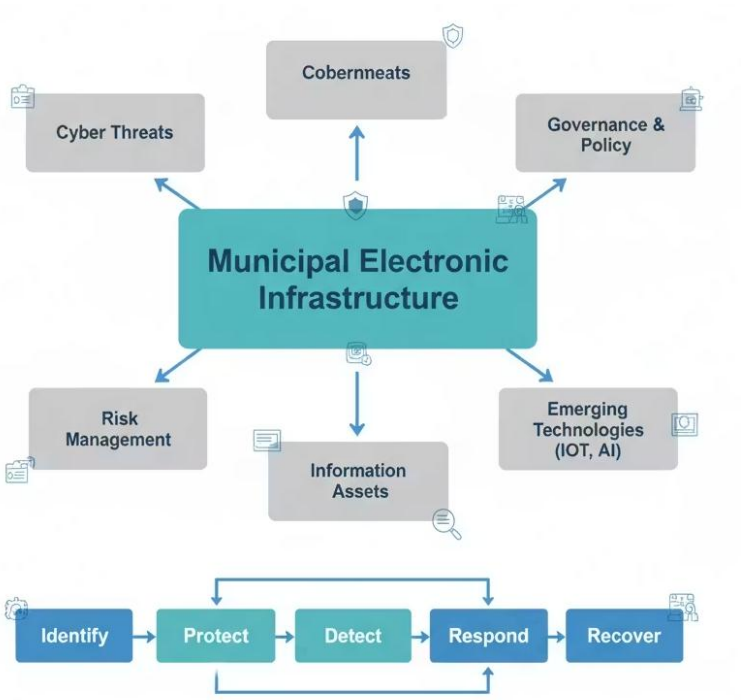
بحران‌های سایبری اخیر در سطح جهان نشان داده‌اند که زیرساخت‌های حیاتی شهری، به دلیل حجم بالای داده‌ها، تنوع سامانه‌ها و پیچیدگی‌های فنی، از آسیب‌پذیرترین اهداف محسوب می‌شوند. حملات باج‌افزاری که شهرهای متعددی را فلج کرده‌اند، نمونه‌ای بارز از این تهدید هستند که مستقیماً بر توانایی دولت محلی برای ارائه خدمات ضروری مانند اورژانس، جمع‌آوری زباله و خدمات آب و فاضلاب تأثیر می‌گذارند. در زمینه ملی، با توجه به اهمیت راهبردی خدمات شهرداری به عنوان نقطه تماس اصلی میان حکومت و شهروندان، ضعف در امنیت اطلاعات می‌تواند نه تنها منجر به اختلال در خدمات شود، بلکه اعتماد عمومی به نهادهای دولتی را نیز به شدت تضعیف کند. عدم وجود یک چارچوب امنیتی مدون، یکپارچه و متناسب با مقیاس و ماهیت فعالیت‌های شهرداری، یکی از چالش‌های بنیادین در این حوزه به شمار می‌رود. بسیاری از شهرداری‌ها در ایران، در فازهای اولیه یا میانی مهاجرت دیجیتال قرار دارند و اغلب رویکردهای امنیتی اتخاذ شده، پراکنده، واکنشی و فاقد انسجام راهبردی هستند (قاسمی، ۲۰۲۴).

بنابراین، مسئله محوری این پژوهش این است که چگونه می‌توان یک چارچوب امنیت اطلاعات (ISF) جامع و مقاوم در برابر تهدیدات نوظهور را برای محیط پیچیده و حساس زیرساخت‌های الکترونیکی شهرداری توسعه داد که ضمن تأمین الزامات قانونی و انطباقی، رویکردی پیشگیرانه و مبتنی بر مدیریت ریسک را در پیش گیرد. این چارچوب باید بتواند توازن دقیقی میان تسهیل نوآوری دیجیتال و حفظ محرمانگی، یکپارچگی و دسترس‌پذیری (CIA) اطلاعات برقرار کند. ضعف در این حوزه، شکافی میان آرمان‌های شهر هوشمند و واقعیت‌های عملیاتی موجود ایجاد می‌کند و توسعه پایدار شهری را به مخاطره می‌اندازد. چارچوب‌های امنیتی عمومی (مانند ISO ۲۷۰۰۱) غالباً چارچوبی کلی ارائه می‌دهند، اما نیاز به تخصصی‌سازی و بومی‌سازی برای الزامات خاص شهرداری‌ها، از جمله تعامل با شهروندان و مدیریت داده‌های مکانی و جمعیتی، ضروری است (صفرزاده و همکاران، ۲۰۲۳).

این مقاله با هدف پاسخگویی به این نیاز مبرم، ساختار جامعی از اجزای لازم برای یک چارچوب امنیت اطلاعات شهرداری را تشریح می‌کند. این چارچوب باید فراتر از ملاحظات صرفاً فنی (مانند فایروال‌ها و آنتی‌ویروس‌ها) عمل کرده و شامل ابعاد حکمرانی، سازمانی، مدیریت ریسک، و پاسخگویی به حوادث باشد. با در نظر گرفتن ظهور فناوری‌هایی مانند اینترنت اشیاء (IoT) در زیرساخت‌های شهری (مانند سنسورهای هوشمند و مدیریت انرژی) و استفاده فزاینده از هوش مصنوعی در تحلیل داده‌های شهری، چارچوب باید پویایی لازم برای دربرگیری این فناوری‌های نوظهور را نیز داشته باشد. نادیده گرفتن این ابعاد منجر به ایجاد نقاط کور امنیتی می‌شود که مهاجمان سایبری می‌توانند از آن‌ها برای نفوذ و ایجاد اختلال استفاده کنند. در این

راستا، رویکرد مدیریتی مبتنی بر ریسک، به عنوان هسته اصلی هر چارچوب موفق امنیتی، باید جایگاه ویژه‌ای بیابد (جوری و همکاران، ۲۰۲۴).

همچنین، پیاده‌سازی موفقیت‌آمیز چنین چارچوبی نیازمند درک عمیقی از وضعیت موجود زیرساخت‌های الکترونیکی در شهرداری‌های ایران است. تجربه نشان داده است که چالش‌هایی مانند کمبود بودجه، فقدان نیروی انسانی متخصص در حوزه امنیت سایبری، و تنوع پلتفرم‌ها و سامانه‌های قدیمی (Legacy Systems)، موانع جدی بر سر راه یکپارچه‌سازی امنیتی هستند. بنابراین، چارچوب پیشنهادی باید قابلیت انطباق با این محدودیت‌های عملیاتی را داشته باشد و بتواند به صورت مرحله‌ای و مبتنی بر اولویت‌بندی ریسک‌ها، پیاده‌سازی شود. تحلیل جامع شکاف میان الزامات استانداردها و وضعیت فعلی شهرداری‌ها، که در بخش‌های بعدی به تفصیل بررسی خواهد شد، مبنای طراحی راهکارهای عملیاتی این چارچوب خواهد بود (عزیزی و همکاران، ۲۰۱۳). از منظر حکمرانی، امنیت اطلاعات نباید صرفاً یک دغدغه فنی تلقی شود، بلکه باید به عنوان یک جزء اساسی از استراتژی کلان مدیریت شهری و شفافیت آن در نظر گرفته شود. این امر مستلزم تعریف نقش‌ها و مسئولیت‌های مشخص در سطوح عالی مدیریت، از شهردار گرفته تا مدیران فنی و کارمندان عملیاتی است. چارچوب توسعه‌یافته باید مکانیزم‌هایی برای نظارت مستمر بر انطباق، آموزش مستمر کارکنان و گزارش‌دهی شفاف در مورد وضعیت امنیتی به ذی‌نفعان (از جمله شورای شهر و شهروندان) فراهم آورد. این رویکرد حکمرانی، تضمین می‌کند که سرمایه‌گذاری‌ها در حوزه امنیت، همسو با اهداف استراتژیک سازمان بوده و صرفاً به عنوان یک هزینه دیده نشوند (رضایی صدرآبادی و همکاران، ۲۰۲۵). به طور خلاصه، عدم وجود یک سند راهبردی مدون و بومی‌سازی شده برای امنیت اطلاعات در شهرداری‌ها، به مثابه یک ریسک سیستمی عمل می‌کند که می‌تواند بهره‌وری حاصل از سرمایه‌گذاری‌های هنگفت در حوزه شهر هوشمند را به خطر اندازد. این پژوهش با هدف پر کردن این خلأ، به بررسی عمیق ساختارها، تهدیدات و الزامات پرداخته و چارچوبی را پیشنهاد می‌دهد که نقش محوری در تقویت تاب‌آوری سایبری (Cyber Resilience) سازمان‌های شهری ایفا کند. چارچوب پیشنهادی قرار است ابزاری مدیریتی برای هدایت تصمیم‌گیری‌ها، تخصیص منابع و سنجش عملکرد در حوزه امنیت اطلاعات باشد تا اطمینان حاصل شود که خدمات حیاتی شهری در برابر هرگونه نفوذ یا اختلال، پایدار باقی می‌مانند.



شکل ۱. مدل مفهومی امنیت اطلاعات زیرساخت‌های الکترونیکی شهرداری با تأکید بر تهدیدات سایبری نوظهور. این مدل تعامل میان زیرساخت الکترونیکی شهرداری، دارایی‌های اطلاعاتی، فناوری‌های نوظهور، الزامات حکمرانی و تهدیدات سایبری را در چارچوب چرخه مدیریت امنیت اطلاعات مبتنی بر استاندارد NIST نشان می‌دهد.

مدل مفهومی ارائه‌شده در این شکل، زیرساخت‌های الکترونیکی شهرداری را به‌عنوان هسته مرکزی اکوسیستم امنیت اطلاعات در نظر می‌گیرد و نشان می‌دهد که این زیرساخت‌ها به‌طور هم‌زمان تحت تأثیر عوامل متعددی از جمله حکمرانی و سیاست‌گذاری امنیتی، مدیریت ریسک، دارایی‌های اطلاعاتی، فناوری‌های نوظهور نظیر اینترنت اشیا و هوش مصنوعی، و طیف گسترده‌ای از تهدیدات سایبری قرار دارند. در بخش پایینی مدل، چرخه پنج‌مرحله‌ای امنیت سایبری شامل شناسایی (Identify)، حفاظت (Protect)، تشخیص (Detect)، پاسخ (Respond) و بازیابی (Recover) به‌عنوان چارچوب عملیاتی مدیریت امنیت اطلاعات نمایش داده شده است که به‌صورت پیوسته و چرخه‌ای عمل می‌کند. این چرخه بیانگر گذار از رویکردهای واکنشی و مقطعی به سمت رویکردی نظام‌مند، پیشگیرانه و تاب‌آور در مدیریت امنیت اطلاعات شهرداری‌هاست. مدل حاضر تأکید می‌کند که اثربخشی امنیت سایبری زمانی محقق می‌شود که ملاحظات فنی، مدیریتی و راهبردی به‌صورت یکپارچه در ساختار حکمرانی دیجیتال شهری لحاظ شوند.

۲: مبانی نظری و مفهومی امنیت اطلاعات در زیرساخت‌های الکترونیکی شهرداری

مفهوم امنیت اطلاعات در بستر شهرداری‌های الکترونیکی، فراتر از حفاظت از دارایی‌های فناوری اطلاعات (IT) است و ابعاد گسترده‌تری از حکمرانی داده‌ها، پایداری خدمات و اطمینان شهروندان را در بر می‌گیرد. امنیت اطلاعات در این محیط‌ها، به مجموعه‌ای از تدابیر مدیریتی، فنی و فیزیکی اطلاق می‌شود که هدف آن‌ها تضمین سه اصل بنیادین محرمانگی (Confidentiality)، یکپارچگی (Integrity) و دسترس‌پذیری (Availability) اطلاعات (CIA Triad) در طول چرخه حیات

داده‌ها است. با این حال، در محیط شهری دیجیتال، این سه اصل باید با ملاحظات ویژه‌ای تفسیر شوند؛ محرمانگی داده‌های شخصی شهروندان (مانند سوابق مالیاتی یا شناسنامه)، یکپارچگی داده‌های مربوط به زیرساخت‌های فیزیکی (مانند اطلاعات نقشه‌برداری شهری یا وضعیت شبکه برق) و دسترس‌پذیری مستمر خدمات حیاتی (مانند اورژانس شهری و سیستم‌های ترافیکی)، از اهمیت حیاتی برخوردارند (قربانی و همکاران، ۲۰۱۶).

چارچوب‌های امنیت اطلاعات، به عنوان مدل‌های ساختاریافته، فرآیندهایی را برای مدیریت ریسک‌های امنیتی در یک سازمان تعریف می‌کنند. در سطح جهانی، چارچوب‌هایی مانند خانواده استاندارد ISO/IEC ۲۷۰۰۰، چارچوب NIST Cybersecurity Framework (CSF)، و COBIT، به عنوان مبنای طراحی راهبردهای امنیتی عمل می‌کنند. هر یک از این چارچوب‌ها دیدگاهی متفاوت را ارائه می‌دهند؛ ISO ۲۷۰۰۱ بر سیستم مدیریت امنیت اطلاعات (ISMS) تمرکز دارد، NIST CSF بر شناسایی، حفاظت، تشخیص، واکنش و بازیابی تأکید می‌کند، و COBIT بیشتر بر همسویی فناوری اطلاعات با اهداف کسب‌وکار (که در اینجا خدمات شهری است) تمرکز دارد. برای شهرداری‌ها، تلفیق این رویکردها ضروری است تا هم انطباق با استانداردهای بین‌المللی حاصل شود و هم اهداف عملیاتی حاکمیت محلی تأمین گردد (مومنی و همکاران، ۲۰۲۳).

پیچیدگی زیرساخت‌های شهرداری ناشی از گستردگی و تنوع سامانه‌های مورد استفاده است. این سامانه‌ها شامل سیستم‌های مدیریت ارتباط با مشتری (CRM)، سیستم‌های اطلاعات جغرافیایی (GIS)، سامانه‌های مالی و اداری، و اخیراً پلتفرم‌های شهر هوشمند مبتنی بر اینترنت اشیاء (IoT) هستند. این تنوع، منجر به ایجاد «سطح حمله» (Attack Surface) بسیار بزرگی می‌شود که مدیریت آن نیازمند یک رویکرد «دفاع در عمق» (Defense in Depth) است. دفاع در عمق به معنای ایجاد لایه‌های متعددی از کنترل‌های امنیتی است، به طوری که شکست هر لایه، لایه بعدی بتواند مانع از نفوذ کامل شود. این لایه‌ها شامل کنترل‌های فیزیکی، کنترل‌های محیطی شبکه، کنترل‌های نرم‌افزاری و در نهایت کنترل‌های مدیریتی و رویه‌ای هستند (علیخانی و همکاران، ۲۰۱۷). یکی از مفاهیم کلیدی در چارچوب‌های نوین، تمرکز بر «تاب‌آوری سایبری» (Cyber Resilience) به جای صرفاً «پیشگیری» است. پذیرش این واقعیت که وقوع یک نفوذ در نهایت اجتناب‌ناپذیر است، دیدگاه مدیریتی را از تمرکز صرف بر مسدودسازی حملات به سمت قابلیت بازیابی سریع و تداوم کسب‌وکار تغییر می‌دهد. برای شهرداری‌ها، تاب‌آوری سایبری به معنای توانایی حفظ حداقل سطح عملکردی خدمات ضروری شهری حتی در مواجهه با یک حمله سایبری بزرگ است. این امر مستلزم برنامه‌ریزی قوی برای تداوم کسب‌وکار (BCP) و بازیابی فاجعه (DRP) است که باید به طور منظم در محیط‌های عملیاتی شبیه‌سازی و مورد آزمایش قرار گیرند (زینالی عظیم و همکاران، ۲۰۲۴).

حکمرانی امنیت اطلاعات (Security Governance) به عنوان پارادایم اصلی در سطح رهبری برای حمایت از چارچوب امنیتی مطرح می‌شود. حکمرانی امنیت اطلاعات اطمینان حاصل می‌کند که استراتژی‌های امنیتی با اهداف کسب‌وکار سازمان (یعنی ارائه خدمات کارآمد شهری) همسو هستند و منابع به طور مؤثر تخصیص داده می‌شوند. این امر مستلزم ایجاد یک ساختار سازمانی مشخص برای امنیت، از جمله تعیین افسر ارشد امنیت اطلاعات (CISO) یا معادل آن در ساختار شهرداری، و همچنین تعریف معیارهای سنجش عملکرد امنیتی (KPIs) است. بدون حمایت رهبری و یکپارچگی حکمرانی، تلاش‌های فنی اغلب به اقدامات مقطعی و ناکارآمد تبدیل می‌شوند (رضایی صدرآبادی و همکاران، ۲۰۲۵). مفهوم ریسک در محیط شهری دیجیتال نیز چندوجهی است. ریسک‌های سایبری مستقیماً بر ریسک‌های عملیاتی (مانند توقف سامانه‌های کنترل ترافیک)، ریسک‌های مالی (هزینه‌های بازیابی و احتمالی جریمه‌ها)، و ریسک‌های اعتباری (از دست دادن اعتماد شهروندان) تأثیر می‌گذارند. چارچوب‌های امنیت اطلاعات باید شامل یک فرآیند رسمی مدیریت ریسک باشند که شامل شناسایی دارایی‌های حیاتی (Critical Assets)، ارزیابی تهدیدات و آسیب‌پذیری‌ها، محاسبه سطح ریسک و اجرای کنترل‌های متناسب برای کاهش ریسک تا سطح قابل قبول

سازمانی (Risk Appetite) است. این فرآیند باید به طور چرخه‌ای و بر اساس تغییرات محیط فناوری و تهدیدات تکرار شود (جوری و همکاران، ۲۰۲۴). در نهایت، بُعد انسانی و فرهنگی در امنیت اطلاعات شهرداری‌ها اغلب نادیده گرفته می‌شود، اما به دلیل تعامل گسترده کارمندان با سامانه‌های مختلف و حجم بالای داده‌های حساس، حیاتی است. مفهوم «پیچیدگی انسانی» به عنوان بزرگترین آسیب‌پذیری در نظر گرفته می‌شود. چارچوب باید شامل برنامه‌های جامع آموزش آگاهی‌بخشی امنیتی باشد که کارکنان را در مورد مهندسی اجتماعی، تشخیص فیشینگ و اهمیت حفاظت از اطلاعات آموزش دهد. همچنین، فرهنگ‌سازی برای گزارش‌دهی سریع حوادث امنیتی، به عنوان یک عنصر کلیدی در تشخیص زودهنگام تهدیدات، باید نهادینه شود (روستایی و همکاران، ۲۰۱۸).

۳: مروری نظام‌مند بر زیرساخت‌های الکترونیکی و سامانه‌های دیجیتال شهرداری‌ها در ایران

زیرساخت‌های الکترونیکی شهرداری‌ها در ایران، طی دو دهه گذشته شاهد رشد چشمگیری بوده‌اند و از سامانه‌های سنتی مبتنی بر اسناد کاغذی به سمت پلتفرم‌های متمرکز و غیرمتمرکز دیجیتال حرکت کرده‌اند. این تحول، که غالباً تحت عنوان دولت الکترونیک یا شهر هوشمند دنبال می‌شود، شامل مجموعه‌ای ناهمگون از سامانه‌هاست که هر کدام نیازمندی‌های امنیتی خاص خود را دارند. هسته اصلی این زیرساخت‌ها معمولاً شامل سامانه‌های متمرکز مدیریت اطلاعات شهری (مانند GIS شهری)، سیستم‌های مالی و اداری (مانند یکپارچه‌سازی با سامانه مالی دولت)، پورتال‌های خدمات شهروندی (مانند سامانه پرداخت عوارض و صدور مجوز) و شبکه‌های ارتباطی داخلی و خارجی است. تنوع این سامانه‌ها و نحوه تعامل آن‌ها با یکدیگر، چالش‌های امنیتی خاصی را ایجاد می‌کند (عزیزی و همکاران، ۲۰۱۳). یکی از مشخصه‌های اصلی زیرساخت‌های شهرداری در ایران، وجود سامانه‌های قدیمی (Legacy Systems) در کنار سامانه‌های نوین است. بسیاری از شهرداری‌ها، به ویژه در حوزه‌های مالی و مدیریت اسناد، از نرم‌افزارهای قدیمی و سفارشی‌سازی شده‌ای استفاده می‌کنند که یا پشتیبانی فنی مستقلی ندارند یا بر بستر فناوری‌های منسوخ شده اجرا می‌شوند. این سامانه‌های قدیمی معمولاً فاقد مکانیزم‌های امنیتی مدرن بوده، به‌روزرسانی وصله‌های امنیتی آن‌ها دشوار یا پرهزینه است، و به دلیل عدم انطباق با معماری‌های مدرن شبکه، به نقاط ورود آسان برای مهاجمان تبدیل می‌شوند. این وضعیت، یکپارچگی امنیتی کل شبکه را به پایین‌ترین سطح ممکن کاهش می‌دهد (قاسمی، ۲۰۲۴).

در حوزه ارتباطات و شبکه‌ها، شهرداری‌ها در تلاش برای ایجاد شبکه‌های ارتباطی اختصاصی (مانند شبکه‌های فیبر نوری یا VPNهای سازمانی) هستند تا تبادل داده‌ها بین مناطق مختلف شهری و ستاد مرکزی را به صورت امن برقرار سازند. با این حال، وابستگی به زیرساخت‌های عمومی اینترنت و استفاده از اینترنت اشیاء شهری (مانند دوربین‌های نظارتی یا سنسورهای محیطی) که اغلب از امنیت ضعیفی برخوردارند، ریسک نفوذ را افزایش می‌دهد. سامانه‌های IoT، به دلیل محدودیت‌های سخت‌افزاری در نصب رمزنگاری‌های قوی و عدم امکان به‌روزرسانی منظم، به عنوان دروازه‌های ضعیف در محیط شبکه عمل می‌کنند، که این امر مورد توجه جدی در چارچوب‌های امنیتی نوین قرار گرفته است (مرادزاده و همکاران، ۲۰۲۲). داده‌ها، به عنوان ارزشمندترین دارایی یک شهرداری الکترونیکی، شامل اطلاعات مکانی دقیق، داده‌های تراکنش‌های مالی شهروندان و سوابق هویتی آن‌ها هستند. مدیریت این داده‌ها با چالش‌هایی نظیر نبود طبقه‌بندی دقیق داده‌ها (Data Classification) و عدم اجرای سخت‌گیرانه سیاست‌های حفظ حریم خصوصی مواجه است. متأسفانه، در بسیاری از موارد، داده‌های حساس بدون رمزنگاری مناسب در حال انتقال یا ذخیره‌سازی هستند، که در صورت وقوع نفوذ، منجر به نقض گسترده حریم خصوصی شهروندان خواهد شد (صفرزاده و همکاران، ۲۰۲۳). این امر نیازمند پیاده‌سازی یک سیستم مدیریت اطلاعات امن (SMS) است که بر اساس ارزش و حساسیت داده‌ها، کنترل‌های حفاظتی لازم را اعمال کند (ضیاءپور و نقی‌زاده، ۲۰۲۲).

حکمرانی امنیت اطلاعات در شهرداری‌های ایران غالباً متمرکز بر جنبه‌های انطباق با قوانین بالادستی (مانند قوانین حفاظت از داده‌های ملی) است، اما فاقد ساختارهای مدیریتی قوی برای اجرای مستمر و نظارت بر آن‌ها است. سازماندهی تیم‌های امنیتی اغلب به صورت متمرکز در سطح فناوری اطلاعات تعریف می‌شود و کمتر به ساختارهای امنیتی چندلایه که شامل نمایندگانی از بخش‌های عملیاتی (مانند ترافیک یا مالی) باشد، توجه می‌شود. این ساختار، اجرای سیاست‌های امنیتی را به وظیفه‌ای صرفاً فنی تقلیل می‌دهد و مانع از پذیرش مسئولیت امنیتی در سطوح مدیریتی بالاتر می‌شود (رضایی صدرآبادی و همکاران، ۲۰۲۵). تأکید بر توسعه سامانه‌های شهر هوشمند، نیازمند معماری‌های توزیع‌شده و مبتنی بر فضای ابری (Cloud Computing) است. در حالی که برخی شهرداری‌ها به سمت استفاده از زیرساخت ابری حرکت کرده‌اند، این انتقال معمولاً با ابهاماتی در خصوص مالکیت، محل ذخیره‌سازی داده‌ها و مسئولیت‌های امنیتی مشترک همراه است. عدم تعریف دقیق مسئولیت‌های امنیتی میان شهرداری و ارائه‌دهندگان خدمات ابری (Cloud Service Providers)، می‌تواند منجر به ایجاد «شکاف‌های امنیتی» شود که مورد سوءاستفاده مهاجمان قرار می‌گیرند (جوری و همکاران، ۲۰۲۴).

آسیب‌پذیری‌های سازمانی نیز در زیرساخت‌های ایران مشهود است. فقدان بودجه کافی برای ارتقای مستمر سخت‌افزارها و نرم‌افزارها، کمبود نیروی انسانی متخصص در حوزه امنیت سایبری که توانایی مدیریت و تحلیل داده‌های امنیتی را داشته باشند، و همچنین نوسانات در اولویت‌بندی پروژه‌ها توسط مدیریت‌های شهری، همگی مانع از استقرار یک رویکرد امنیتی پایدار می‌شوند. این عوامل دست به دست هم داده و زیرساخت‌های دیجیتال شهرداری را در برابر تهدیدات پیچیده، بسیار آسیب‌پذیر می‌سازند (قربانی و همکاران، ۲۰۱۶). در نهایت، مروری بر وضعیت فعلی نشان می‌دهد که زیرساخت‌های الکترونیکی شهرداری‌ها در ایران، علی‌رغم پیشرفت‌های چشمگیر در ارائه خدمات، هنوز فاقد یک چارچوب امنیتی جامع، یکپارچه و مبتنی بر ریسک هستند که بتواند پیچیدگی‌های فنی و الزامات حکمرانی را در برابر تهدیدات سایبری نوظهور برآورده سازد. این شکاف، ضرورت توسعه چارچوبی تخصصی را که در بخش‌های بعدی مقاله معرفی خواهد شد، تأیید می‌کند (صفرزاده و همکاران، ۲۰۲۳).

۴: تهدیدات سایبری نوظهور علیه شهرداری‌ها

با تکامل زیرساخت‌های الکترونیکی شهرداری‌ها به سمت مدل‌های شهر هوشمند و افزایش اتکا به اینترنت اشیاء و داده‌های کلان، نوع و شدت تهدیدات سایبری نیز به طور چشمگیری تغییر یافته و پیچیده‌تر شده است. تهدیدات نوظهور دیگر صرفاً شامل نفوذهای ساده یا حملات DOS (انکار سرویس) نیستند، بلکه حملاتی هدفمند، مخرب و با انگیزه مالی یا سیاسی را شامل می‌شوند که می‌توانند زیرساخت‌های حیاتی شهری را به طور کامل فلج سازند. شناخت دقیق این تهدیدات، پیش‌نیاز اصلی برای توسعه یک چارچوب امنیتی مقاوم است (مرادزاده و همکاران، ۲۰۲۲). یکی از برجسته‌ترین تهدیدات نوظهور، حملات باج‌افزاری (Ransomware) پیشرفته است. مهاجمان با استفاده از تکنیک‌های مهندسی اجتماعی پیچیده یا بهره‌برداری از آسیب‌پذیری‌های روز صفر (Zero-day)، به شبکه نفوذ کرده و علاوه بر رمزگذاری فایل‌ها و دیتابیس‌های حیاتی (مانند سوابق شهروندان و اطلاعات مالیاتی)، اقدام به «باج‌گیری مضاعف» (Double Extortion) می‌کنند؛ یعنی داده‌ها را سرقت کرده و در ازای عدم انتشار، درخواست باج می‌کنند. شهرداری‌ها به دلیل حساسیت بالای داده‌هایشان و فشار عمومی برای بازگرداندن خدمات، اهداف ایده‌آلی برای این حملات محسوب می‌شوند. مقابله با این تهدید نیازمند راهکارهایی فراتر از آنتی‌ویروس‌ها، از جمله سیستم‌های تشخیص و پاسخ نقطه پایانی (EDR) و استراتژی‌های پشتیبان‌گیری ایزوله (Immutable Backups) است (زینالی عظیم و همکاران، ۲۰۲۴).

حملات زنجیره تأمین (Supply Chain Attacks) یکی دیگر از مسیرهای نفوذ پرخطر هستند. در معماری‌های شهری دیجیتال، شهرداری‌ها به شدت به فروشندگان نرم‌افزاری، پیمانکاران نگهداری سیستم‌ها و ارائه‌دهندگان خدمات ابری وابسته هستند. نفوذ به یکی از این شرکای مورد اعتماد و تزریق کدهای مخرب به نرم‌افزارهای آن‌ها (مانند به‌روزرسانی‌های جعلی)، امکان نفوذ به شبکه‌های داخلی شهرداری را فراهم می‌آورد بدون اینکه کنترل‌های امنیتی ورودی اصلی فعال شوند. چارچوب امنیتی باید شامل یک برنامه سخت‌گیرانه مدیریت ریسک تأمین‌کنندگان (Third-Party Risk Management) باشد که امنیت تأمین‌کنندگان را به طور مداوم ممیزی کند (جوری و همکاران، ۲۰۲۴). تهدیدات مرتبط با اینترنت اشیاء (IoT) در شهر هوشمند، یک بعد کاملاً جدید را به تهدیدات اضافه کرده‌اند. میلیون‌ها سنسور، دوربین، و دستگاه کنترلی هوشمند در شبکه شهری متصل می‌شوند. متأسفانه، بسیاری از این دستگاه‌ها با پیکربندی‌های پیش‌فرض امنیتی ضعیف، رمزهای عبور سخت (Hardcoded Passwords) و فقدان قابلیت وصله‌پذیری اجرا می‌شوند. یک مهاجم می‌تواند با تصرف تعداد زیادی از این دستگاه‌ها، یک بات‌نت (Botnet) قدرتمند تشکیل دهد و از آن‌ها برای اجرای حملات DDoS با حجم بالا علیه سامانه‌های حیاتی شهرداری یا زیرساخت‌های ملی استفاده کند. همچنین، دستکاری داده‌های سنسورها (مانند اطلاعات ترافیکی یا حسگرهای محیطی) می‌تواند منجر به تصمیم‌گیری‌های مدیریتی غلط و ناخواسته شود (مرادزاده و همکاران، ۲۰۲۲).

استفاده از هوش مصنوعی (AI) و یادگیری ماشین (ML) در تحلیل داده‌های شهری، در کنار مزایای فراوان، مسیرهای جدیدی برای سوءاستفاده مخرب باز کرده است. تهدیدات مبتنی بر هوش مصنوعی شامل «تولید محتوای متقاعدکننده فیشینگ» (Deepfake Phishing) برای فریب مدیران، یا حملات «سمی کردن داده‌ها» (Data Poisoning) است که در آن مهاجمان داده‌های جعلی و مغرضانه را به مجموعه آموزشی مدل‌های هوشمند شهرداری تزریق می‌کنند تا خروجی مدل‌ها را در راستای اهداف خود تغییر دهند (مثلاً تغییر تخصیص منابع یا تصمیمات صدور پروانه). مقابله با این حملات نیازمند رویکردهای امنیتی پیشرفته‌تر، مانند امنیت مبتنی بر ناهنجاری (Anomaly-Based Security) و راستی‌آزمایی مدل‌های هوش مصنوعی است (رضایی صدرآبادی و همکاران، ۲۰۲۵).

حملات هدفمند علیه APIها (رابط‌های برنامه‌نویسی کاربردی) که پل ارتباطی بین سامانه‌های مختلف و سرویس‌های خارجی هستند، نیز اهمیت فزاینده‌ای یافته‌اند. از آنجا که سامانه‌های شهرداری در حال تعامل بیشتر با اپلیکیشن‌های موبایلی شهروندان و سایر سازمان‌ها هستند، APIها به نقاط ورودی حیاتی تبدیل شده‌اند. ضعف در اعتبارسنجی ورودی‌ها، مدیریت ضعیف توکن‌های دسترسی یا افشای اطلاعات در پاسخ‌های API، می‌تواند به مهاجم اجازه دهد تا به کل پایگاه داده دسترسی یابد. چارچوب باید شامل یک برنامه دقیق برای مدیریت چرخه عمر APIهای امنیتی باشد (صفرزاده و همکاران، ۲۰۲۳). علاوه بر تهدیدات فنی، تهدیدات ناشی از «جاسوسی سایبری دولتی» (State-Sponsored Cyber Espionage) نیز بر سازمان‌های دولتی و نیمه‌دولتی مانند شهرداری‌ها سایه افکنده است. این مهاجمان معمولاً از منابع نامحدود برخوردار بوده و هدفشان نفوذ بلندمدت، سرقت اطلاعات استراتژیک شهری (مانند نقشه‌های زیرساختی) یا ایجاد قابلیت‌های اختلال در زمان بحران است. این حملات نیازمند سطوح بالایی از قابلیت تشخیص و پاسخگویی است که فراتر از ابزارهای امنیتی استاندارد عمل کند و بر تحلیل رفتاری (Behavioral Analysis) متمرکز باشد (علیخانی و همکاران، ۲۰۱۷). در نهایت، تهدیدات ناشی از فعالیت‌های داخلی (Insider Threats)، خواه با نیت مخرب و خواه ناشی از سهل‌انگاری، همواره پابرجا هستند. کارکنان شهرداری به دلیل دسترسی گسترده به سامانه‌های حیاتی، در صورت قرار گرفتن در معرض فیشینگ یا داشتن سوءنیت، می‌توانند آسیب‌پذیری‌های جدی ایجاد کنند. تهدیدات نوظهور مانند استفاده از ابزارهای هوش مصنوعی برای خودکارسازی حملات داخلی و دور زدن کنترل‌های سنتی، نیازمند رویکردهای قوی‌تر مبتنی بر اصل «کمترین امتیاز» (Least Privilege) و نظارت مستمر بر رفتار کاربران ویژه (UEBA) است تا بتوان فعالیت‌های غیرعادی را در مراحل اولیه شناسایی کرد (قربانی و همکاران، ۲۰۱۶).

۵: آسیب‌پذیری‌های فنی، سازمانی و مدیریتی در ساختار امنیت اطلاعات شهرداری‌ها

آسیب‌پذیری‌ها در ساختار امنیت اطلاعات شهرداری‌ها ریشه در سه حوزه اصلی دارند: فنی، سازمانی و مدیریتی. درک این آسیب‌پذیری‌ها برای تدوین راهکارهای مؤثر در چارچوب پیشنهادی ضروری است. در حوزه فنی، بزرگترین چالش، محیط ناهمگون فناوری و فرسودگی زیرساخت‌هاست. بسیاری از شهرداری‌ها در ایران از ترکیبی از سخت‌افزارهای قدیمی، سیستم‌عامل‌های منسوخ و نرم‌افزارهای سفارشی که مدت‌هاست پشتیبانی نمی‌شوند، استفاده می‌کنند. این سامانه‌های قدیمی، به دلیل عدم امکان نصب وصله‌های امنیتی مدرن، به طور دائم در معرض آسیب‌پذیری‌های شناخته شده‌ای هستند که مهاجمان به راحتی از آن‌ها بهره می‌برند (عزیزی و همکاران، ۲۰۱۳). علاوه بر سامانه‌های قدیمی، آسیب‌پذیری‌های پیکربندی نادرست (Misconfiguration) در زیرساخت‌های نوین نیز رایج است. این امر اغلب در مورد فایروال‌ها، تنظیمات ابری (Cloud Security Posture Management) و به ویژه تجهیزات IoT رخ می‌دهد. دستگاه‌های IoT که بدون تغییر رمز عبور پیش‌فرض نصب می‌شوند، یا پورت‌های مدیریتی که به اشتباه به اینترنت باز می‌مانند، نمونه‌های بارزی هستند که بدون سرمایه‌گذاری کلان، صرفاً با بازنگری در فرآیندهای استقرار می‌توان آن‌ها را اصلاح کرد. نبود رویه‌های سخت‌گیرانه «تأمین امنیت از طراحی» (Security by Design) در پروژه‌های جدید دیجیتال، سبب می‌شود که آسیب‌پذیری‌ها از ابتدا در معماری سیستم‌ها تعبیه شوند (مرادزاده و همکاران، ۲۰۲۲).

در لایه شبکه، ضعف در تقسیم‌بندی (Segmentation) شبکه یکی از آسیب‌پذیری‌های فنی مهم است. در بسیاری از شهرداری‌ها، شبکه فناوری اطلاعات اغلب به صورت یکپارچه (Flat Network) پیکربندی شده است؛ به این معنی که یک نفوذ موفق به یک بخش کم‌اهمیت (مثلاً ایستگاه کاری یک کارمند اداری) می‌تواند به راحتی به بخش‌های حیاتی مانند سرورهای داده‌های شهروندی یا سیستم‌های کنترل زیرساخت‌های فیزیکی (مانند مدیریت روشنایی یا ترافیک) سرایت کند. عدم تفکیک ترافیک عملیاتی (OT) از ترافیک فناوری اطلاعات (IT) در محیط‌های مدرن‌تر، این ریسک را تشدید می‌کند (زینالی عظیم و همکاران، ۲۰۲۴). در حوزه سازمانی، آسیب‌پذیری‌ها عمدتاً در حوزه منابع انسانی و فرآیندها متمرکز هستند. یکی از بزرگترین چالش‌ها، کمبود نیروی انسانی متخصص در حوزه امنیت سایبری است. شهرداری‌ها معمولاً قادر به رقابت با بخش خصوصی در جذب و حفظ کارشناسان امنیت نیستند، که منجر به شکاف مهارتی در تیم‌های داخلی می‌شود. این کمبود مهارت، مانع از استقرار مؤثر ابزارهای پیچیده امنیتی، تحلیل لاگ‌ها (Log Analysis) و انجام ممیزی‌های امنیتی منظم می‌شود (قاسمی، ۲۰۲۴).

همچنین، فقدان فرهنگ امنیتی فراگیر و مستمر در میان کارکنان، یک آسیب‌پذیری سازمانی جدی است. بسیاری از کارکنان، به ویژه کسانی که با سامانه‌های قدیمی کار می‌کنند، اهمیت حفاظت از داده‌ها را درک نمی‌کنند و مستعد افتادن در تله‌های مهندسی اجتماعی هستند. آموزش‌های امنیتی موجود نیز اغلب مقطعی، غیرتخصصی و نامرتبط با تهدیدات روزمره کاری آن‌ها طراحی می‌شوند، که اثربخشی آن‌ها را به شدت کاهش می‌دهد (روستایی و همکاران، ۲۰۱۸). در بعد مدیریتی، ضعف در حکمرانی امنیت اطلاعات یکی از ریشه‌ای‌ترین آسیب‌پذیری‌هاست. این ضعف اغلب به شکل عدم تعریف نقش‌ها و مسئولیت‌های امنیتی واضح (RACI Matrix) بروز می‌کند. در نتیجه، هنگامی که یک حادثه امنیتی رخ می‌دهد، سردرگمی در مورد مرجع تصمیم‌گیری، گزارش‌دهی و مسئولیت نهایی برای مدیریت بحران مشاهده می‌شود. فقدان یک «سند راهبردی امنیت اطلاعات» که توسط بالاترین سطح مدیریت تأیید شده باشد، باعث می‌شود اقدامات امنیتی پراکنده و واکنشی باقی بمانند (رضایی صدرآبادی و همکاران، ۲۰۲۵).

عدم کفایت در فرآیند مدیریت ریسک نیز یک آسیب‌پذیری ساختاری است. بسیاری از شهرداری‌ها ارزیابی‌های ریسک دوره‌ای و جامع انجام نمی‌دهند، یا اگر انجام دهند، نتایج آن در سطح راهبردی مورد توجه قرار نمی‌گیرد و کنترل‌های لازم تخصیص داده نمی‌شوند. این امر به ویژه در مورد ریسک‌های ناشی از فناوری‌های نوظهور مانند فضای ابری و هوش مصنوعی صادق است، جایی که چارچوب‌های مدیریت ریسک سنتی دیگر پاسخگو نیستند (جوری و همکاران، ۲۰۲۴). نهایتاً، ضعف در برنامه‌ریزی تداوم کسب‌وکار و بازیابی از فاجعه (BCP/DRP) یک آسیب‌پذیری بحرانی است. علی‌رغم الزام قانونی برای داشتن طرح‌های بازیابی، بسیاری از شهرداری‌ها این طرح‌ها را فقط به صورت کاغذی نگه داشته و هرگز آن‌ها را در محیط عملیاتی تست نکرده‌اند. در نتیجه، در صورت وقوع حمله سایبری بزرگ، توانایی بازیابی سریع خدمات حیاتی شهری به شدت محدود می‌شود، زیرا فرآیندها، مسئولیت‌ها و منابع مورد نیاز به درستی مشخص و تمرین نشده‌اند (صفرزاده و همکاران، ۲۰۲۳).

۶: چارچوب‌ها، استانداردها و مدل‌های بین‌المللی امنیت اطلاعات و تحلیل قابلیت بومی‌سازی آنها در شهرداری‌های ایران

برای توسعه یک چارچوب امنیت اطلاعات مؤثر، ضروری است که از تجربیات جهانی و استانداردهای معتبر بهره‌برداری شود. چارچوب‌های بین‌المللی مانند NIST Cybersecurity Framework (CSF) و ISO/IEC ۲۷۰۰۱، به عنوان مراجع جهانی برای ایجاد و مدیریت سیستم‌های مدیریت امنیت اطلاعات (ISMS) شناخته می‌شوند. چارچوب NIST CSF با ساختار پنج‌گانه خود (شناسایی، حفاظت، تشخیص، واکنش، بازیابی)، مدلی عملکردگرا ارائه می‌دهد که به‌ویژه برای محیط‌های عملیاتی سریع‌التغییر مانند شهرداری‌های هوشمند مناسب است (قاسمی، ۲۰۲۴). در مقابل، ISO ۲۷۰۰۱ یک رویکرد مبتنی بر مدیریت ریسک سیستماتیک را از طریق الزامات ISMS ارائه می‌دهد که برای تثبیت حکمرانی امنیت اطلاعات ضروری است. قابلیت بومی‌سازی این چارچوب‌ها در بستر شهرداری‌های ایران نیازمند درک چالش‌های بومی است. اگرچه اصول CIA، مدیریت ریسک و کنترل‌های فنی در همه جا یکسان است، اما نحوه اعمال این اصول تحت تأثیر محدودیت‌های بودجه‌ای، پیچیدگی‌های قانونی (مانند الزامات حفاظت از داده‌های ملی) و ساختار مدیریتی خاص سازمان‌های دولتی محلی قرار می‌گیرد. به عنوان مثال، استقرار کامل ISO ۲۷۰۰۱ نیازمند منابع مالی و نیروی انسانی تخصصی بالایی است که اغلب در شهرداری‌ها محدود است؛ لذا، باید رویکردی مرحله‌ای و مبتنی بر بلوغ (Maturity-based Approach) اتخاذ شود (عزیزی و همکاران، ۲۰۱۳).

چارچوب NIST CSF به دلیل انعطاف‌پذیری بالاتر در تعریف سطح بلوغ، می‌تواند نقطه شروع بهتری باشد. شهرداری‌ها می‌توانند ابتدا وضعیت فعلی خود را در مقابل توابع پنج‌گانه NIST ارزیابی کرده و سپس با تعریف سطوح هدف (Target Profile)، نقشه راهی برای بهبود تعیین کنند. این رویکرد اجازه می‌دهد تا سازمان‌هایی که در مراحل اولیه دیجیتالی شدن هستند (سطح شناسایی و حفاظت ضعیف)، تمرکز خود را بر پایه‌ریزی این دو رکن بگذارند، در حالی که شهرداری‌های پیشرفته‌تر می‌توانند تمرکز خود را بر بهبود قابلیت‌های تشخیص و واکنش خودکار قرار دهند (زینالی عظیم و همکاران، ۲۰۲۴). تحلیل انطباق با مقررات محلی نیز بخشی جدایی‌ناپذیر از بومی‌سازی است. چارچوب‌های بین‌المللی باید با الزامات خاص قوانین داخلی ایران در زمینه حفاظت از داده‌ها، امنیت سامانه‌های ملی و الزامات فنی ابلاغی از سوی سازمان‌های ناظر ملی همسو شوند. نادیده گرفتن این الزامات انطباقی، منجر به ریسک‌های قانونی و عملیاتی خواهد شد، حتی اگر از نظر فنی چارچوب بین‌المللی رعایت شده باشد (صفرزاده و همکاران، ۲۰۲۳).

مدل COBIT (به ویژه نسخه‌های اخیر که بر همسویی کسب‌وکار و IT تأکید دارند) می‌تواند به عنوان پلی میان اهداف استراتژیک شهرداری (مانند بهبود خدمات شهروندی) و فعالیت‌های امنیتی عمل کند. این چارچوب کمک می‌کند تا سرمایه‌گذاری‌های

امنیتی مستقیماً به اهداف شهری مرتبط شوند؛ برای مثال، امنیت زیرساخت GIS مستقیماً به هدف "تضمین دقت داده‌های مکانی برای تصمیم‌گیری‌های مدیریتی" مرتبط می‌شود. این پیوند استراتژیک، پشتیبانی مدیریتی لازم را برای موفقیت چارچوب فراهم می‌آورد (مومنی و همکاران، ۲۰۲۳). تجربه نشان داده است که موفقیت در بومی‌سازی چارچوب‌های امنیتی، به جای کپی‌برداری صرف، مستلزم یک فرآیند «تطبیق» (Adaptation) است. این تطبیق باید شامل: ۱) تعریف دارایی‌های حیاتی (Critical Assets) شهری بر اساس تأثیر توقف آن‌ها بر شهروندان، ۲) تعریف ریسک‌های بومی (مانند ریسک‌های ناشی از بلایای طبیعی که ممکن است بر زیرساخت‌های فیزیکی تأثیر بگذارد)، و ۳) در نظر گرفتن محدودیت‌های عملیاتی (مانند پهنای باند محدود یا نیروی کار فنی کم‌تعداد) باشد (قربانی و همکاران، ۲۰۱۶).

رویکرد دیگر، استفاده از مدل‌های مبتنی بر بلوغ مانند Capability Maturity Model Integration (CMMI) در حوزه امنیت است. این مدل‌ها به شهرداری‌ها اجازه می‌دهند تا سطح بلوغ هر کنترل امنیتی (مانند مدیریت وصله یا واکنش به حوادث) را از سطح صفر (وجود ندارد) تا سطح پنج (بهینه‌سازی مستمر) ارزیابی کنند. این ارزیابی به تعیین اولویت‌های سرمایه‌گذاری کمک می‌کند، زیرا منابع محدود ابتدا به سمت کنترل‌هایی هدایت می‌شوند که در پایین‌ترین سطح بلوغ قرار دارند و ریسک سازمانی بالایی را ایجاد می‌کنند (علیخانی و همکاران، ۲۰۱۷). در نهایت، چارچوب‌های بین‌المللی باید به گونه‌ای تفسیر شوند که محوریت «حفاظت از داده‌های عمومی» و «تداوم خدمات حیاتی شهری» را در اولویت قرار دهند. این اولویت‌بندی متفاوت از سازمان‌های مالی یا مخابراتی است؛ در شهرداری، دسترس‌پذیری و یکپارچگی خدمات به اندازه محرمانگی اهمیت دارد. بنابراین، چارچوب پیشنهادی باید یک دیدگاه متعادل بین اصول جهانی و الزامات عملیاتی و اخلاقی خاص حکومت محلی اتخاذ کند (رضایی صدرآبادی و همکاران، ۲۰۲۵).

۷: ارائه چارچوب پیشنهادی جامع امنیت اطلاعات برای زیرساخت‌های الکترونیکی شهرداری با رویکرد راهبردی و عملیاتی

چارچوب پیشنهادی برای امنیت اطلاعات شهرداری‌ها (e-Municipal ISF)، بر اساس تلفیق بهترین عناصر استاندارد NIST CSF (برای رویکرد عملیاتی) و ISO ۲۷۰۰۱ (برای حکمرانی)، و با تمرکز بر بومی‌سازی برای محیط ایران، طراحی شده است. این چارچوب به جای یک سند منفعل، به عنوان یک چرخه مدیریت ریسک فعال و مداوم تعریف می‌شود که در پنج ستون اصلی استوار است: حکمرانی و انطباق، شناسایی و ارزیابی دارایی‌ها، حفاظت فعال، تشخیص و واکنش سریع، و بازیابی و پایداری. این ساختار چندلایه، تضمین می‌کند که ملاحظات امنیتی در تمام مراحل چرخه عمر فناوری و خدمات شهری ادغام می‌شوند (Security by Design) (صفرزاده و همکاران، ۲۰۲۳).

۱. ستون اول: حکمرانی امنیت اطلاعات (Security Governance Compliance): این ستون، سطح راهبردی چارچوب را تشکیل می‌دهد و باید توسط بالاترین مدیریت (شهردار و معاونین) هدایت شود. این بخش شامل ایجاد یک کمیته عالی امنیت سایبری با حضور مدیران ارشد عملیاتی است که مسئولیت نهایی پذیرش ریسک را بر عهده دارند. همچنین، این ستون بر تعریف دقیق سیاست‌های امنیتی جامع، تخصیص بودجه مورد نیاز و اطمینان از انطباق با کلیه الزامات قانونی داخلی و استانداردهای جهانی (به صورت مرحله‌ای) تمرکز دارد. این ستون باید شفافیت در گزارش‌دهی امنیتی به شورای شهر را نیز تضمین کند (رضایی صدرآبادی و همکاران، ۲۰۲۵).

۲. ستون دوم: شناسایی و ارزیابی دارایی‌ها (Asset Identification Risk Assessment): این بخش به عنوان پایه و اساس چارچوب عمل می‌کند و بر اصل «نمی‌توان از آنچه نمی‌دانید محافظت کرد» استوار است. در این مرحله، تمام دارایی‌های فناوری اطلاعات (سرورها، نرم‌افزارها، داده‌ها، APIها و سامانه‌های IoT) باید فهرست‌برداری و طبقه‌بندی شوند. طبقه‌بندی داده‌ها بر اساس حساسیت (عمومی، داخلی، محرمانه) و حیاتی بودن خدمات (بر اساس تأثیر توقف بر شهروندان) انجام می‌شود. پس از شناسایی، فرآیند مدیریت ریسک شامل ارزیابی تهدیدات نوظهور (مانند باج‌افزارها و حملات زنجیره تأمین) علیه این دارایی‌ها و تعیین سطح ریسک قابل قبول (Risk Appetite) شهرداری صورت می‌گیرد (جوری و همکاران، ۲۰۲۴).

۳. ستون سوم: حفاظت فعال (Proactive Protection): این ستون شامل اجرای کنترل‌های امنیتی فنی و رویه‌ای برای کاهش ریسک‌های شناسایی شده است. در بُعد فنی، این شامل پیاده‌سازی دفاع در عمق است: تقسیم‌بندی شبکه (Network Segmentation) برای ایزوله کردن سیستم‌های حیاتی، اجرای مکانیزم‌های قوی کنترل دسترسی مبتنی بر اصل کمترین امتیاز (RBAC/Least Privilege)، رمزنگاری قوی برای داده‌ها در حال سکون و انتقال، و مدیریت آسیب‌پذیری‌ها (Patch Management) به صورت مستمر. در بُعد انسانی، این شامل برنامه‌های آموزش آگاهی‌بخشی مستمر برای مقابله با مهندسی اجتماعی و همچنین ایجاد فرآیندهای امن برای استقرار سامانه‌های جدید (Security by Design) است (قربانی و همکاران، ۲۰۱۶).

٤. ستون چهارم: تشخیص و واکنش سریع (Detection Rapid Response): با توجه به ماهیت تهدیدات نوظهور، انتظار توقف کامل نفوذ وجود ندارد؛ لذا، قابلیت تشخیص زودهنگام حیاتی است. این ستون بر استقرار ابزارهایی مانند SIEM (Security Information and Event Management) برای جمع‌آوری و تحلیل متمرکز لاگ‌ها، و استفاده از UEBA برای تشخیص رفتارهای ناهنجار در شبکه تمرکز دارد. در صورت وقوع حادثه، وجود یک طرح پاسخ به حادثه (Incident Response Plan - IRP) که به صورت مدون، نقش‌ها (تیم واکنش سریع)، مراحل و ابزارهای مورد نیاز برای مهار و ریشه‌کنی نفوذ را مشخص کرده باشد، الزامی است. این طرح باید به طور منظم شبیه‌سازی و تمرین شود (زینالی عظیم و همکاران، ۲۰۲۴).

٥. ستون پنجم: بازیابی و پایداری (Resilience Recovery): این ستون تضمین‌کننده تداوم خدمات شهری است. این امر شامل توسعه و آزمایش مستمر برنامه‌های بازیابی فاجعه (DRP) و تداوم کسب‌وکار (BCP) است که به طور خاص بر بازگرداندن خدمات حیاتی (مانند سیستم‌های آب، ترافیک و اورژانس) در اولویت قرار دهند. سیاست‌های پشتیبان‌گیری باید شامل نسخه‌های ایزوله و غیرقابل تغییر (Immutable) برای مقابله با حملات باج‌افزاری باشد. پس از بازیابی، فرآیند «درس‌آموزی از حادثه» (Lessons Learned) باید اجرا شود تا کنترل‌ها بر اساس یافته‌های واقعی ارتقا یابند و چرخه‌ی چارچوب به سطح بالاتر بلوغ بازگردد (علیخانی و همکاران، ۲۰۱۷). این رویکرد چرخه‌ای، چارچوبی پویا و پاسخگو به محیط متغیر تهدیدات سایبری فراهم می‌آورد.

نتیجه‌گیری، پیامدهای مدیریتی، پیشنهادهای اجرایی و مسیرهای پژوهشی آتی

در پایان این پژوهش، توسعه یک چارچوب امنیت اطلاعات جامع، یک ضرورت استراتژیک برای شهرداری‌هایی است که مسیر تحول دیجیتال را طی می‌کنند. یافته‌های این مقاله تأکید می‌کنند که رویکردهای امنیتی سنتی و پراکنده دیگر پاسخگوی

تهدیدات سایبری نوظهوری چون باج‌افزارها، حملات زنجیره تأمین و چالش‌های امنیتی اینترنت اشیاء نیستند. چارچوب پیشنهادی مبتنی بر پنج ستون کلیدی (حکمرانی، شناسایی ریسک، حفاظت، تشخیص و بازیابی) که از استانداردهای جهانی الهام گرفته و برای محیط عملیاتی شهرداری‌های ایران بومی‌سازی شده است، می‌تواند زیربنای محکمی برای تقویت تاب‌آوری سایبری سازمان‌های شهری فراهم آورد (قاسمی، ۲۰۲۴). پیامدهای مدیریتی: موفقیت این چارچوب به تغییر پارادایم مدیریتی وابسته است. مدیران شهری باید امنیت اطلاعات را نه به عنوان یک هزینه یا یک وظیفه فنی، بلکه به عنوان یک ریسک مدیریتی در سطح کلان بپذیرند. این پذیرش مستلزم تعهد مالی برای به‌روزرسانی سامانه‌های قدیمی، سرمایه‌گذاری در آموزش نیروی انسانی و مهم‌تر از همه، اعطای اختیارات کافی به واحد امنیت سایبری (CISO یا معادل آن) برای اجرای سیاست‌های امنیتی در تمامی بخش‌های عملیاتی است. شفاف‌سازی نقش‌ها و مسئولیت‌ها در سطح هیئت مدیره و مدیران عملیاتی، می‌تواند از شکاف‌های حکمرانی که در بخش پنجم شناسایی شدند، جلوگیری کند (رضایی صدرآبادی و همکاران، ۲۰۲۵).

پیشنهادهای اجرایی: برای پیاده‌سازی مرحله‌ای چارچوب، شهرداری‌ها باید بر اساس مدل بلوغ پیشنهادی، ابتدا بر تقویت ستون‌های اول (حکمرانی) و دوم (شناسایی دارایی‌های حیاتی) تمرکز کنند. اولویت‌بندی باید بر اساس دارایی‌هایی باشد که در صورت اختلال، بیشترین تأثیر را بر خدمات ضروری شهروندان دارند. پیشنهاد می‌شود که پروژه‌هایی نظیر: ۱) پیاده‌سازی یکپارچه رمزنگاری برای دیتابیس‌های شهروندی، ۲) ایجاد تقسیم‌بندی دقیق شبکه برای ایزوله کردن سامانه‌های SCADA و IoT، و ۳) تمرین منظم سناریوهای باج‌افزاری با همکاری تیم‌های پشتیبان‌گیری، به عنوان اقدامات فوری در نظر گرفته شوند (صفرزاده و همکاران، ۲۰۲۳). همچنین، توسعه یک برنامه جامع مدیریت ریسک تأمین‌کنندگان جهت کاهش آسیب‌پذیری‌های زنجیره تأمین حیاتی است (جوری و همکاران، ۲۰۲۴).

مسیرهای پژوهشی آتی: پژوهش‌های آینده باید بر کمی‌سازی تأثیر تهدیدات نوظهور بر شاخص‌های کلیدی عملکرد شهری (KPIs) متمرکز شوند؛ به عنوان مثال، چگونه یک حمله سایبری بر زمان پاسخگویی اورژانس شهری تأثیر می‌گذارد. همچنین، توسعه یک مدل اندازه‌گیری بلوغ امنیتی خاص برای محیط‌های شهرداری ایران که محدودیت‌های منابع را در نظر بگیرد، می‌تواند ابزار مدیریتی قدرتمندی فراهم آورد. بررسی نقش و مکانیسم‌های دفاع سایبری مبتنی بر هوش مصنوعی در محیط‌های شهری و تدوین پروتکل‌های امنیتی برای تعاملات بین سامانه‌های IoT شهری با یکدیگر، از دیگر مسیرهای مهم پژوهشی هستند (مرادزاده و همکاران، ۲۰۲۲). چارچوب ارائه شده در این مقاله، نه یک نقطه پایانی، بلکه نقطه عزیمت برای این بهبودهای مستمر و پژوهش‌های عمیق‌تر در حوزه امنیت سایبری حکمرانی شهری است (روستایی و همکاران، ۲۰۱۸).

منابع

- اسکندری ثانی محمد, مرادی محمود, قادری مقدم پروین. (۲۰۱۸). ارزیابی پتانسیل های پیاده سازی شهر هوشمند با تأکید بر حمل ونقل، موردمطالعه: شهر بیرجند.
- امیرحسین قاسمی. (۲۰۲۴). پتانسیل سنجی استقرار شهر هوشمند مبتنی بر اینترنت اشیا، با تمرکز بر زندگی هوشمند (مطالعه موردی: شهربیرجند). توسعه پایدار و ساختمان هوشمند, ۱(۳), ۱۹-۳۶.
- باقری, محمدی زاده, ماریا. (۲۰۱۷). رتبه‌بندی جاذبه‌های اکوتوریسمی شهرستان جاسک با استفاده از روش تصمیم‌گیری چند معیاره (MCDM). فصلنامه جغرافیا (برنامه ریزی منطقه ای), ۶(۲۵), ۷-۱۶.
- جووری, بهنوش, یگانگی, سید کامران. (۲۰۲۴). زیرساخت های الکترونیکی در خدمت مدیریت منابع انسانی شهرداری ها. مطالعات مدیریت خدمات عمومی, ۲(۳).

- رضایی صدرآبادی نجمه, معین زاد حسین, کرامتی محمدعلی. (۲۰۲۵). طراحی مدل پیش بینی رفتار زنجیره تامین پویا خدمات الکترونیک شهری (مطالعه موردی: شهرداری ناحیه تاریخی یزد).
- رضائی صدرآبادی, معین زاد, کرامتی. (۲۰۲۵). طراحی مدل پیش‌بینی رفتار زنجیرهٔ تأمین پویا خدمات الکترونیک شهری (مطالعهٔ موردی: شهرداری ناحیهٔ تاریخی یزد). مطالعات میان‌رشته‌ای معماری ایران, ۴(۷), ۱۱۷-۱۴۳.
- روستایی, دکتر شهریور, پورمحمدی, قنبری. (۲۰۱۸). تئوری شهر هوشمند و ارزیابی مؤلفه‌های زیرساختی آن در مدیریت شهری مورد شناسی: شهرداری تبریز. جغرافیا و آمایش شهری منطقه‌ای, ۸(۲۶), ۱۹۷-۲۱۶.
- زینالی عظیم, فدائی حقی, مهری, علیزاده, امین, جدیری عباسی, ... شریفی. (۲۰۲۴). سنجش عوامل موثر در عدم توسعه شهر هوشمند پایدار تبریز. فصلنامه علوم محیطی, ۲۲(۳), ۴۲۷-۴۴۶.
- سعید مظفری, حمزه کریمی. (۲۰۲۲). شناسایی و دسته بندی تکنیک های تصمیم گیری چند معیاره گسسته (MADM) با استفاده از روش های MCDM. نشریه علمی رویکردهای پژوهشی نوین مدیریت و حسابداری, ۴(۱۴), ۱۱۵-۱۳۳.
- سلماسی, سهرابی, رهبر, محمدی, حیدر. (۲۰۲۰). مطالعه امکان‌سنجی کسب وکار نوپا تفکیک از مبدأ و جمع‌آوری پسماند جامد شهری قابل بازیافت با استفاده از فناوری دیجیتال: مطالعه موردی شهر همدان. اقتصاد شهری, ۵(۲), ۱۳۵-۱۴۸.
- شریفی, یوسفعلی, جلالی, عبدالعلی, ضرغامی. (۲۰۲۴). شناسایی و اولویت بندی روش های روسازی سطوح پروازی فرودگاه های ایران با استفاده از تکنیک های تصمیم گیری چند معیاره (MCDM). نشریه علمی پژوهشی مهندسی هوانوردی, ۲۶(۱), ۲۷-۴۱.
- صفرزاده, بازایی, قاسمعلی, فقیهی. (۲۰۲۳). مدل‌سازی عوامل فنی مؤثر بر پیاده‌سازی طرح‌های شهر هوشمند با استفاده از رویکرد مدل‌سازی تفسیری ساختاری. اقتصاد و برنامه ریزی شهری, ۴(۲), ۱۹۲-۲۰۸.
- عزیزی, شهریار, صفائی فراهانی, روناک. (۲۰۱۳). ارزیابی آمادگی الکترونیکی شهرداری تهران. چشم انداز مدیریت دولتی, ۳(۳).
- علیخانی, ناجی عظیمی, لگزیان. (۲۰۱۷). ارزیابی آمادگی الکترونیکی مناطق شهرداری مشهد در راستای تحقق شهرداری الکترونیک. چشم انداز مدیریت دولتی, ۸(۳), ۸۷-۱۰۸.
- قربانی, سرمست, بهزام, مهدی پور. (۲۰۱۶). بررسی زیرساختهای استقرار شهرداری الکترونیک در کلان شهر تبریز. مدیریت سازمان‌های دولتی, ۴(شماره ۲ (پیاپی ۱۴)), ۱۳۷-۱۴۸.
- مرادزاده, علی, دریوش, مبارک‌پور, فربد, بحری, ... صدیق‌اصرافی. (۲۰۲۲). مدیریت شهری الکترونیک؛ از برنامه ریزی تا اجرا. پژوهشهای جدید در مدیریت و حسابداری, ۸۲(۸), ۳۵-۴۴.
- مرادی, متولیگله کلائی, نظامی اصل سیسی, سیف السادات. (۲۰۲۴). چالش‌های پیاده‌سازی مدیریت شهر هوشمند در حوزه حمل‌ونقل همگانی ایران. پژوهشنامه پردازش و مدیریت اطلاعات, ۴۰(۱), ۷۱-۹۲.
- مومنی, کورش, ملکی, حسنی‌سیاه‌گلی, دامن‌باغ, صفیه. (۲۰۲۳). اولویت‌بندی موانع و چالش‌های پیش‌روی شهر هوشمند در شهر اهواز. مدیریت شهری و روستایی, ۷۱(۲۱), ۲۳-۳۵.
- مهرداد ضیاءپور, رضا نقی‌زاده کوچصفهانی. (۲۰۲۲). مروری بر تکنیک‌های پرکاربرد داده‌کاوی جهت تصمیم‌گیری مدیران شهرداری در حوزه مدیریت شهری. نشریه علمی رویکردهای پژوهشی نوین مدیریت و حسابداری, ۵(۱۶), ۲۶۲-۲۸۰.