مزیت‌های معماری سازمانی در برخورد با تهدیدهای امنیت سایبری و ریسک‌های تجاری

علیرضا مقدسی[۱]، علی محجوبی[۲]

[۱]استادیار، گروه مدیریت، دانشگاه بین‌المللی امام رضا (علیه السلام)، مشهد
alireza.moghadasi@imamreza.ac.ir
[۲]دانشجوی کارشناسی ارشد، مرکز آموزش الکترونیکی، دانشگاه فردوسی مشهد
alimahjoubi.1990@gmail.com

چکیده

معماری سازمانی نقش حیاتی در کاهش جامع ریسک‌های تجاری و تضمین مقاومت سازمان در برابر تهدیدات امنیت سایبری دارد. این مطالعه بر اهمیت معماری سازمانی در ساختارهای سازمانی معاصر و تأثیر آن بر این مسائل تأکید می‌کند، به‌خصوص در زمانی که تهدیدات امنیت سایبری در سکونتگاه تجاری جهانی بیشتر و بیشتر می‌شوند. با ادغام منابع انسانی، چارچوب‌های حکمرانی، فناوری و فرایندها، معماری سازمانی دیدگاه جامعی از محیط فناوری اطلاعات را در سازمان ارائه می‌دهد. با استفاده از یک چارچوب حکمرانی روشمند، معماری سازمانی بررسی‌های جامعی از وابستگی‌ها بین اجزا انجام می‌دهد، آسیب‌پذیری‌ها را شناسایی می‌کند و پایه‌های قوی برای پیشگیری بهبودیافته از تهدیدات فراهم می‌آورد. معماری سازمانی نه‌تنها ابزار مدیریت پیشگیری از ریسک است، بلکه به طراحی کلی استراتژی تجاری نیز به‌طور قابل توجهی کمک می‌کند. ادغام امنیت سایبری و معماری سازمانی نه‌تنها به تقویت زیرساخت فناوری کمک می‌کند، بلکه آن را به استراتژی کلی کسب‌وکار متصل می‌کند و این امکان را فراهم می‌آورد که تلاش‌های امنیت سایبری با اهداف سازمان هم‌راز شوند، ازاین‌رو با استراتژی کسب‌وکار ارتباط برقرار کنند. ادغام امنیت سایبری و معماری سازمانی نه‌تنها به تقویت زیرساخت‌های فناوری کمک می‌کند، بلکه آن را به استراتژی کلی کسب‌وکار متصل می‌سازد و این امکان را فراهم می‌کند که تلاش‌های امنیت سایبری با اهداف سازمان هم‌راستا شوند و با استراتژی کسب‌وکار همگام شوند. این مطالعه بر توانایی ادغام پاسخ‌های سریع و چابک به تهدیدات، به فرهنگ سازمانی تأکید می‌کند تا نوآوری را تقویت کند. به‌عنوان کاتالیست استراتژیک، به سازمان‌ها کمک می‌کند تا با تهدیدات سایبری سازگار شوند، منافع تجاری را حفاظت کنند و عملکردهای خود را در یک محیط دیجیتال پویا بهینه کنند. با ادغام چارچوب‌های حکمرانی و معماری سازمانی، سازمان‌ها می‌توانند به‌طور پیشگیرانه ریسک‌های تجاری و تهدیدات امنیت سایبری را کاهش دهند و مقاومت و پایداری را در محیط دیجیتال پویا تقویت کنند.

کلمات کلیدی: فرهنگ سازمانی، امنیت سایبری، معماری سازمانی، کسب و کار جهانی، مدیریت ریسک.

۱ مقدمه

دوران دیجیتال امروزی چالش منحصر به فردی را به دلیل پیشرفت‌های فناورانه و گسترش چشمگیر مناظر تهدیدات سایبری برای کسب‌وکارها در انواع صنایع به وجود آورده است. ظهور تهدیدات سایبری پیچیده و چندلایه‌ای باعث شده است که سازمان‌ها به بازنگری استراتژی‌های خود مجبور شوند. معماری سازمانی به عنوان پایه‌ای برای ساخت سیستم‌های اطلاعاتی سازمانی تبدیل شده است تا دفاع‌های سازمانی را تقویت کرده و مدیریت ریسک‌های کسب‌وکار را در پاسخ به این مسأله فوری بهبود بخشد. مکانیسم‌های دفاعی سنتی در برابر حملات سایبری پیچیده و فراوان، آسیب‌پذیر هستند. نفوذ به داده‌ها، حملات رنسومور، و تخریب سیستم‌ها عملیات را قطع کرده و اعتماد ذی‌نفعان را به خطر می‌اندازد. در برابر تهدیداتی که به سرعت تغییر می‌کنند، رویکردهای سایبری جدا و واکنشی باید بهبود یابند. برای مقابله با این تهدیدات در حال تکامل، کسب‌وکارها به یک سیستم جامع و پیشگیرانه نیاز دارند که فناوری، فرآیندها و عوامل انسانی را یکپارچه کند.

معماری سازمانی به‌طور مداوم به عنوان یک عنصر بحرانی در امنیت سایبری شناخته می‌شود (هیندارتو و همکاران، ۲۰۲۱). این معماری، اهداف کسب‌وکار و استراتژی فناوری اطلاعات را سازماندهی می‌کند تا به سازمان‌ها کمک کند منظره فناوری خود را درک کنند (آماندا و همکاران، ۲۰۲۳؛ ایسواهیودی و همکاران، ۲۰۲۳). معماری سازمانی با نشان دادن روابط و وابستگی‌های اجزا، به سازمان‌ها کمک می‌کند تا آسیب‌پذیری‌ها را شناسایی کرده و دفاع‌ها را تقویت کند. ظرفیت کامل معماری سازمانی در مقابله با تهدیدات امنیت سایبری و ریسک‌های کسب‌وکار نیاز به بررسی و بررسی بیشتری دارد. هدف این پژوهش به نمایش گذاشتن آن است که چگونه روش‌های معماری سازمانی می‌توانند در کاهش تهدیدات امنیت سایبری و مدیریت ریسک‌های کسب‌وکار در پاسخ به مشکلات موجود کمک کنند. این مطالعه ادغام استراتژیک اصول معماری سازمانی در سازمان‌ها را برای شناسایی مزایا و معایب بررسی می‌کند. در مرحله بعد، عوامل بحرانی را که می‌توانند معماری سازمانی را به عنوان یک دفاع سایبری پیشگیرانه استفاده کنند در حالی که اهداف کسب‌وکار را برآورده می‌کنند، شناسایی کند (هیندارتو، ۲۰۲۳).

همانطور که فراوانی و پیچیدگی تهدیدات امنیت سایبری افزایش می‌یابد، مکانیسم‌های دفاع سنتی آسیب‌پذیر شده‌اند. نفوذ به سیستم‌ها، حملات رنسومر و نفوذ به داده‌ها نه تنها عملیات را قطع بلکه اعتماد ذی‌نفعان را نیز خدشه‌دار می‌کنند. سازمان‌ها به رویکردی پیشگیرانه و جامع نیاز دارند که عوامل انسانی، فرآیندها و فناوری را هماهنگ تا در برابر این تهدیدات پیوسته‌ی متغیر محافظت کند. حملات نرم‌افزارهای مخرب، نشت اطلاعات و دزدی داده‌ها مثال‌هایی از تهدیدات سایبری هستند که به‌طور قابل توجهی عملیات کسب‌وکار را مختل کرده‌اند (هیندارتو و سانتوسو، ۲۰۲۱، ۲۰۲۲) و به دلیل این حوادث، اعتماد افراد مرتبط با سازمان، از جمله مشتریان، شرکای تجاری و سایر ذینفعان، خدشه‌دار شده است. استراتژی‌هایی که عمدتاً بر تقویت زیرساخت‌های فناوری اطلاعات و پاسخ به ریسک‌های جدید تمرکز دارند، نیازمند بهبود در مقابله با تهدیدات پیچیده و در حال گسترش هستند.

بنابراین، نیاز به یک استراتژی جامع و پیشگیرانه حس می‌شود. سازمان‌ها نیاز به یک رویکرد استراتژیک

دارند که استفاده مؤثر از فناوری، کنترل دقیق فرآیندها، و درک عمیق از عوامل انسانی را در برگیرد. ادغام مؤثر بین این سه عنصر بسیار حیاتی است زمانی که با تهدیداتی که به طور مداوم در حال تکامل و پیچیده‌تر شدن هستند، روبرو هستیم. با اتخاذ این استراتژی جامع، سازمان‌ها می‌توانند توانایی خود را در مقابله با خطرات سایبری که پیوسته در حال تغییر هستند بهبود بخشند، عملیات بدون وقفه را حفظ کنند، و اعتماد ذی‌نفعان خود را تقویت نمایند.

نقش معماری سازمانی در امنیت سایبری برای سازمان‌ها به طور روزافزون واضح می‌شود (ساری و هیندارتو، ۲۰۲۳). معماری سازمانی از یک رویکرد ساختارمند استفاده می‌کند تا اهداف کسب‌وکار را با استراتژی‌های فناوری اطلاعات هم‌راستا کند و به سازمان‌ها در درک چشم‌انداز فناوری خود کمک نماید. معماری سازمانی با تعریف روابط اجزا و وابستگی‌ها، به سازمان‌ها کمک می‌کند آسیب‌پذیری‌ها را شناسایی کرده و دفاع‌ها را تقویت کند. با این حال، ظرفیت کامل معماری سازمانی در مقابله با تهدیدات امنیت سایبری و ریسک‌های کسب‌وکار نیاز به بررسی بیشتری دارد.

هدف اصلی این مطالعه بررسی اثربخشی معماری سازمانی در افزایش توانایی‌های امنیت سایبری سازمان در همزمان با کاهش ریسک‌های کسب‌وکار مرتبط است. علاوه بر این، مطالعه حاضر به بررسی موانع اصلی می‌پردازد که در استقرار معماری سازمانی برای کاهش خطرات سایبری مواجه می‌شوند. هدف این مطالعه تجزیه و تحلیل چالش‌ها و پیچیدگی‌هایی است که سازمان‌ها در هنگام ادغام معماری سازمانی به چارچوب امنیت سایبری خود مواجه می‌شوند. علاوه بر این، تلاش می‌شود تا موانعی که در پیاده‌سازی سریع و بدون مشکل معماری سازمانی وجود دارد، شناسایی و شرح داده شود. سؤالات تحقیق به شرح زیر می‌باشند:

- سؤال پژوهش ۱: چه روش‌ها و عوامل ضروری در ادغام معماری سازمانی برای مدیریت جامع امنیت سایبری وجود دارند؟
- سؤال پژوهش ۲: چه تأثیری دارد هم‌آرا کردن معماری سازمانی با اهداف کسب‌وکار بر افزایش توانایی مقابله با تهدیدات سایبری جدید؟

این تحقیق به دنبال ارتقاء دانش و تفکر در خصوص استفاده از طراحی نقشه یا معماری سازمانی به‌عنوان یک رویکرد استراتژیک برای مواجهه با منظره تهدیدات سایبری پیوسته در حال تکامل است. نوآوری اینجاست که به طور جامع بررسی می‌شود که چگونه معماری سازمانی، نه تنها به عنوان یک تقویت فناوری، بلکه به عنوان یک امکان‌ساز استراتژی‌های کسب‌وکار مقاوم در برابر خطرات سایبری عمل می‌کند. این بخش مقدمه‌ای را برای بررسی عمیق استفاده استراتژیک از معماری سازمانی در مقابله با تهدیدات امنیت سایبری و مدیریت ریسک‌های کسب‌وکار می‌گذارد، با هدف کشف بینش‌هایی که به شکل استراتژی‌های سازمانی مقاوم و سازگار کمک می‌کنند.

۲ روش‌شناسی

تعدادی از مراحل اساسی برای ایجاد یک سامانه سازمان‌مند و مؤثر باید پیگیری شوند. گام اول در درک پایه مفهومی و اصول راهنمایی توسعه سامانه شامل انجام یک مرور جامع از ادبیات مربوط است. این مرحله به گروه ارزیابی شده عمق فهمی از شیوه‌های عملیاتی موفق را که در محیط‌های مشابه آزمایش شده‌اند، می‌دهد. از طریق استفاده از نظرسنجی‌ها و مصاحبه‌ها، فهم جامع‌تری از ذی‌نفعان به‌دست آید. با برقراری ارتباط مستقیم با آنها، می‌توان نیازها، انتظارات و موانع آنها را تشخیص داد و سپس به‌عنوان پایه برای توسعه راه‌حل‌های مناسب خدمت کرد. برگزاری جلسات با همه ذی‌نفعان مربوطه برای اطمینان از اینکه همه با اهداف مشترک توسعه سامانه، دامنه و نیازمندی‌ها موافق هستند، انجام می‌شود. ارتباط مؤثر در این زمینه بسیار حیاتی است زیرا تضمین می‌کند که تمامی طرف‌ها هدف یکسانی داشته باشند و انتظارات خود را هماهنگ کنند. پس از این، معماری برنامه کاربردی پیشنهادی طراحی می‌شود. این مرحله شامل توسعه یک چارچوب جامع، انتخاب فناوری مناسب و تعیین ساختار کلی برنامه است. سپس، معماری زیرساخت و اجرا دقیقاً طراحی می‌شود. حضور زیرساخت قوی و اجرای کارآمد، مؤلفه‌های ضروری برای عملکرد بی‌درنگ برنامه‌ها هستند. مرحله ارزیابی معماری با بررسی و تأیید می‌کند که هر عنصر از معماری طراحی شده، الزامات عملکردی و غیرعملکردی مشخص شده را به درستی ارضا کرده و با اهداف کلی توسعه سامانه سازگار است. جمعاً، این مراحل مهم پایه‌ای را در ساخت یک سامانه سازمان‌مند، یکپارچه و کارآمد تشکیل می‌دهند.

۱.۲ امنیت سایبری

امنیت سایبری به‌عنوان مانع اصلی در برابر مجموعه‌ای از خطرات که در دامنه دیجیتال پنهان هستند، عمل می‌کند. این ساختار شامل یک وب پیچیده از روش‌ها، نصب‌ها و کنترل‌ها است که از اطلاعات حساس سیستم‌ها و شبکه‌ها در برابر نهادهای شرور حفاظت می‌کند. در دوران فعلی جهانی‌شدن و تعامل بین دستگاه‌ها، جایی که جریان داده‌ها به راحتی بین کشورها و دستگاه‌ها انجام می‌شود، اهمیت امنیت سایبری نمی‌تواند به طور زیادی نادیده گرفته شود. این پدیده به عنوان یک مکانیسم دفاعی اساسی عمل می‌کند که دولت‌ها، سازمان‌ها و افراد را در برابر مجموعه گسترده‌ای از تهدیدات سایبری، شامل اقدامات هک پیچیده، حملات رنسوم‌ور و تلاش‌های فیشینگ و غیره محافظت می‌کند. هدف اصلی تقویت دسترسی‌پذیری، محرمانگی و صحت سیستم‌ها و داده‌هاست، و این‌گونه تضمین می‌شود که عملیات آنها در مقابل نیروهای مخالف پایدار باشد.

رشد دائمی امنیت سایبری نمایانگر ویژگی‌های پیوسته تغییر کننده‌ی محیط دیجیتال است که سعی در حفاظت از آن دارد. به علت پیچیدگی و پیشرفت مداوم تهدیدات سایبری، استراتژی‌های امنیت سایبری باید به طور مداوم سازگار و پیشرفت کنند. به دست آوردن این موضوع نیازمند یک رویکرد جامع است که شامل مدیریت پیشگیرانه ریسک، پروتکل‌های امنیتی مقاوم، نظارت مداوم و مکانیسم‌های پاسخ سریع به حوادث است. علاوه بر این که یک مسئله فناورانه است، امنیت سایبری یک زمینه مطالعاتی است که شامل رفتار انسانی، فرآیندها، سیاست‌ها و فناوری می‌شود. این فرآیند نیازمند یک هم‌بندی قوی بین فناوری‌های

شکل ۱: روش‌شناسی

پیشرفته شامل هوش مصنوعی، سیستم‌های شناسایی نفوذ، رمزنگاری، سیاست‌های جامع، آموزش کارکنان و یک محیط سازمانی است که به مقاومت سایبری اهمیت می‌دهد، می‌باشد. اهمیت امنیت سایبری فراتر از موجودیت‌های فردی است و یک جزء بحرانی از امنیت ملی و پایداری جهانی را تشکیل می‌دهد. حملات سایبری قابلیت ایجاد آشوب گسترده، تخریب داده‌های دولتی محرمانه و مختل کردن زیرساخت‌های حیاتی جهانی را دارند. بنابراین، دولت‌ها، بخش خصوصی و نهادهای بین‌المللی باید به همکاری با یکدیگر بپردازند تا یک چارچوب مقاوم را برای تبادل اطلاعات تهدید و مقابله با تهدیدات سایبری به وجود آورند. به طور اساسی، امنیت سایبری به عنوان یک سنگ بنای ضروری دوران دیجیتال عمل می‌کند که اعتماد و پایداری سیستم‌های پیونددهنده با پیوندهای همه‌گیر، اقتصادها و ارتباطات بین‌المللی ما را تضمین می‌کند. توسعه و تنظیم مداوم امری ضروری برای حفظ اعتماد، ثبات و حفاظت در دامنه دیجیتال است.

۲.۲ سامانه تشخیص و پیشگیری از تجاوز

با گسترش امنیت سایبری، سیستم تشخیص و پیشگیری از تجاوز (IDPS)[1] به عنوان یک عنصر حیاتی در حفاظت از سیستم‌های کامپیوتری و شبکه‌ها به شمار می‌رود. هدف اصلی این سیستم شناسایی، پیشگیری و پاسخگویی به حملاتی است که ممکن است امنیت زیرساخت دیجیتال را به خطر بیاندازد یا آسیبی به آن وارد

[1] Intrusion Detection and Prevention System (IDPS)

کند. وظیفه اصلی سیستم تشخیص و پیشگیری از تجاوز شناسایی فعالیت‌های مشکوک در ترافیک داده‌های وارد و خارج شده از شبکه است که به صورت مداوم هشدار داده و یا اقداماتی انجام می‌دهد تا خطرات امنیتی را کاهش دهد. سیستم تشخیص و پیشگیری از تجاوز به عنوان یک ناظر پیش‌بین، فعالیت‌های شبکه، سیستم و داده را مشاهده کرده و به پیش‌بینی حملات محتمل می‌پردازد. این شامل حملات سایبری است که سعی در نفوذ به یک سیستم را دارند، و همچنین حملات انکار سرویس توزیع‌شده (DDoS)[۲] که با استفاده از تکنیک‌های متنوع شناسایی نشانه‌های حمله، بررسی فعالیت‌های غیرمعمول، و نظارت بر الگوهای ترافیک شبکه، سعی در شناسایی و پیشگیری از تجاوز دارند و هدف آن مدیریت سریع تهدیدات است. در مجموع، سیستم تشخیص و پیشگیری از تجاوز نقش اساسی در شناسایی سریع و مدیریت تهدیدات سایبری، از جمله حملات به سیستم‌ها یا مخدوش کردن خدمات توسط حملات انکار سرویس توزیع شده، ایفا می‌کند و به حفظ امنیت و سلامت زیرساخت‌های دیجیتال در منظر بهداشت سایبری امروزی کمک زیادی می‌کند.

نوع‌های اصلی سیستم‌های تشخیص و پیشگیری از تجاوز شامل سیستم تشخیص (IDS)[۳] و پیشگیری نفوذ (IPS)[۴] هستند. سیستم تشخیص نفوذ به هدف شناسایی فعالیت‌های مشکوک یا نقض‌های امنیتی می‌پردازد و این امکان را فراهم می‌کند که هشدارها به مدیران سیستم داده شود تا برای اقدامات بعدی آماده شوند. این دو عنصر به همکاری برای ایجاد یک حافظه قوی و قابل تطبیق در برابر تهدیدات سایبری متغیر کمک می‌کنند. این کار با بررسی ترافیک شبکه و لاگ‌های فعالیت برای شناسایی الگوهای غیرمعمول که ممکن است نشانگر یک نفوذ باشند، انجام می‌شود. بالعکس، سیستم پیشگیری نفوذ نسبت به سیستم تشخیص نفوذ قابلیت‌های پیشگیری، علاوه بر قابلیت‌های شناسایی مشابه سیستم تشخیص نفوذ بهبود یافته‌ای دارد. با وقفه در انتقال داده‌های شناسایی شده به عنوان تهدید یا با به‌طور خودکار تغییر دادن قوانین دسترسی، سیستم پیشگیری نفوذ می‌تواند اقدامات سریعی را برای پیشگیری یا مسدود سازی حملات شناسایی شده انجام دهد.

وظیفه اصلی سیستم‌های تشخیص و پیشگیری از تجاوز نظارت بر ترافیک شبکه و فعالیت‌های سیستم به صورت زمان واقعی است. این نیازمند مشاهده جریان داده، بسته‌های ارسالی و دریافتی، و یک مجموعه متنوعی از پارامترهای شبکه است. سیستم تشخیص و پیشگیری از تجاوز با استفاده از روش‌ها و تکنیک‌هایی از جمله تشخیص رفتار (بر پایه رفتار)، تشخیص ناهنجاری (بر پایه ناهنجاری) و روش‌ها و تکنیک‌های بر پایه امضا، حملات یا رفتارهای مشکوک را شناسایی می‌کند. تشخیص رفتاری سعی در شناسایی فعالیت‌های نامتعارف نشان داده شده توسط کاربران یا سیستم‌ها دارد، در حالی که روش‌های امضا الگوهای حمله‌ای که شناخته شده‌اند را با ترافیک فعلی مقایسه می‌کنند. بلعکس از این موارد، تشخیص ناهنجاری الگوهای معمول ترافیک را نظارت می‌کند و در صورت شناسایی فعالیت ناهنجار، اعلان می‌سازد. پیاده‌سازی یک سیستم تشخیص و پیشگیری از تجاوز برای حفاظت از زیرساخت‌های فناوری اطلاعات در برابر تهدیدات سایبری حیاتی است. با استفاده از رویکرد دوگانه تشخیص و پیشگیری، سیستم‌های تشخیص و پیشگیری

[2]Distributed Denial-of-Service
[3]Intrusion Detection System
[4]Intrusion Detection System

از تجاوز به حفظ امنیت سیستم و شبکه کمک می‌کنند و از تهدیداتی که به صورت پیوسته و به تدریج پیچیده می‌شوند، حفاظت می‌کنند. با اینکه سیستم تشخیص و پیشگیری از تجاوز نقش اساسی در حفاظت از زیرساخت‌های دیجیتال را دارد، با چندین مشکل نیز روبه‌رو می‌شود. این شامل مسئله احتمال بروز مثبت‌های غلط یا منفی‌های غلط است که ممکن است دقت تشخیص تهدید را کاهش دهد. به علاوه، نگهداری مداوم و پیکربندی‌های پیچیده باید در نظر گرفته شوند هنگامی که سعی می‌شود که عملکرد سیستم تشخیص و پیشگیری از تجاوز بهینه‌سازی شود.

۳.۲ معماری سازمانی

معماری سازمانی بر پایه چارچوب معماری گروه باز (TOGAF)[۵]، به عنوان یک رویکرد ساختارمند و جامع در توسعه معماری سازمانی شناخته می‌شود. چارچوب معماری گروه باز راهنمای جامعی را در تهیه، پیاده‌سازی و مدیریت معماری ارائه می‌دهد که شامل جنبه‌های تجاری و فناوری می‌شود. این چارچوب از چندین فرایند، روش شناسایی و ابزار تشکیل شده است که طراحی و توسعه معماری را که به نیازهای سازمانی بپردازد، پشتیبانی می‌کند. یکی از ویژگی‌های کلیدی چارچوب معماری گروه باز ، دوره چرخه‌ای ساختارمند و بازگشتی آن است. این دوره به چندین مرحله تقسیم می‌شود که شامل درک نیازهای تجاری، توسعه معماری، پیاده‌سازی راه حل و نظارت و به‌روزرسانی مداوم می‌باشد. با این رویکرد، سازمان‌ها می‌توانند نیازهای تجاری خود را بهتر درک کنند و یک معماری که اهداف استراتژیک را پشتیبانی می‌کند توسعه دهند و اطمینان حاصل کنند که پیاده‌سازی به‌طور مؤثر صورت می‌گیرد و معماری را به نیازهای در حال تغییر تطبیق دهند.

چارچوب معماری گروه باز همچنین انعطاف‌پذیری در پیاده‌سازی خود ارائه می‌دهد. این چارچوب می‌تواند به نیازهای خاص یک سازمان سازگار شود بدون اینکه از اصالت و ساختار اساسی خود کاسته شود. این امکان را برای سازمان‌ها فراهم می‌کند که بخش‌های خاصی از چارچوب معماری گروه باز را که بیشترین ارتباط و ملایمت را با وضعیت خود دارد، به‌کار بگیرند بدون اینکه مجبور باشند کل چارچوب را دنبال کنند، که قابلیت سفارشی‌سازی معماری را برای تطبیق با شرایط داخلی و خارجی سازمان فراهم می‌آورد. یکی از مزایای اصلی چارچوب معماری گروه باز توجه به توازن بین جنبه‌های تجاری و فناورانه است. با در نظر گرفتن جنبه‌های تجاری مانند استراتژی، فرآیندها و نیازهای مشتری به همراه فناوری استفاده‌شده، چارچوب معماری گروه باز به سازمان‌ها امکان می‌دهد تا معماری‌هایی را طراحی کنند که نه تنها عملیات فعلی را پشتیبانی می‌کنند بلکه سازمان را برای رشد و سازگاری در آینده آماده می‌سازند. به طور کلی، چارچوب معماری گروه باز یک مفهوم سازمان‌مند و سیستماتیک را به توسعه معماری سازمانی می‌آورد. از طریق رویکرد مکرر و انعطاف‌پذیر خود و توجه متوازن به جنبه‌های تجاری و فناوری، چارچوب معماری گروه باز راهنمای قدرتمندی برای طراحی، مدیریت و به‌روزرسانی معماری‌هایی فراهم می‌کند که پایدار بوده و به نیازهای متغیر تجاری پاسخ می‌دهند.

دوره‌ی مرتب‌سازی‌شده‌ی چارچوب معماری گروه باز به عنوان یک اجزای بنیادی شناخته می‌شود.

[5] The Open Group Architecture Framework (TOGAF)

این چارچوب شامل چهار حوزه اصلی است، به‌ویژه تعیین اهداف معماری، پیشرفت طراحی معماری، اجرای برنامه‌های معماری و نظارت بر عملیات معماری است. این چارچوب رویکرد سیستماتیکی را برای نظارت و هدایت بهینه‌ی پیشرفت یک چارچوب معماری جامع در یک محیط سازمانی فراهم می‌آورد. فرایند با درک جامع اهداف و نیازهای تجاری آغاز می‌شود، سپس با فرمول‌بندی یک چارچوب معماری مناسب ادامه می‌یابد. و راه‌حل‌های برنامه‌ریزی شده اجرا می‌شوند و یک چرخه مداوم از نظارت و به‌روزرسانی آغاز می‌شود تا تطابق با پیشرفت‌های سازمانی و فناورانه تضمین شود. چارچوب معماری گروه باز همچنین ساختاری بسیار انعطاف‌پذیر فراهم می‌آورد. این امکان را به سازمان‌ها می‌دهد که فرایند معماری را به طور مؤثری تغییر دهند و با روش‌ها یا راه‌های موجود دیگر ادغام کنند. طراحی ماژولار چارچوب به استفاده از اجزای انتخابی اجازه می‌دهد بدون این که نیاز به پذیرش ساختار کلی داشته باشد. این ویژگی انعطاف‌پذیری مورد نیاز را برای سفارشی‌سازی معماری به تطابق با نیازهای خاص یک سازمان فراهم می‌آورد.

چارچوب معماری گروه باز تأکید قابل توجهی بر روی دوام و توازن میان ملاحظات تجاری و فناوری دارد. یکی از مزایای قابل توجه ارائه شده توسط چارچوب معماری گروه باز ، تأکید بر دستیابی به تعادل هماهنگ بین اهداف تجاری و آرمان‌های فناوری است. این رویکرد به سازمان‌ها امکان می‌دهد که معماری‌هایی را تدوین کنند که نه‌تنها نیازهای کنونی تجاری را برآورده می‌کنند، بلکه سازمان را برای گسترش و تطبیق با پیشرفت‌های فناوری سریع آماده می‌سازند. چارچوب معماری گروه باز با به‌کارگیری یک رویکرد متعادل برای مدیریت ملاحظات تجاری و فناوری، توسعه معماری‌های قابل تداوم و مقیاس‌پذیر برای سازمان‌ها را تسهیل می‌دهد. در نهایت، چارچوب معماری گروه باز برای اجرای شیوه‌ها و بهره‌وری مؤثر منابع را تأییدی می‌کند. چارچوب معماری گروه باز به عنوان یک دستاورد برای اتخاذ استانداردها و منابع جهت طراحی و مدیریت معماری بهینه، تأکید دارد. این امر باعث بهبود استفاده از منابع در سازمان‌ها می‌شود، احتمال اجراهای ناموفق را کاهش می‌دهد، و معماری قابل تطبیق و مقاومی فراهم می‌آورد. به طور کلی، استفاده از چارچوب معماری گروه باز در معماری سازمانی یک ساختار جامع و منظم برای مدیریت معماری سازمانی فراهم می‌آورد. چارچوب معماری گروه باز ابزاری ارزشمند در برنامه‌ریزی، توسعه و مدیریت است که به نیازهای متغیر تجاری و فناوری پاسخ می‌دهد و این را با تأکید بر چرخه‌های فرایند ساختارمند، انعطاف‌پذیری، ایجاد تعادل هماهنگ بین تجارت و فناوری و انتخاب دقیق شیوه‌های بهینه فراهم می‌سازد.

۳ نتایج

۱.۳ معماری برنامه‌ای

این مطالعه نشان می‌دهد که بسیاری از سازمان‌ها نیازمند استراتژی‌های قوی هستند تا از داده‌های خود به‌طور مؤثر محافظت کنند، از جمله راهکارهای پیشگیرانه مانند نظارت امنیتی و اجرای سیستم‌های شناسایی نفوذ و عدم آمادگی در برابر حملات سایبری باعث می‌شود که سازمان‌ها به صورت واکنشی عمل کنند و نیاز به سیستم‌های بیشتری برای شناسایی و پیشگیری از تهدیدات داشته باشند. این چارچوب، مطالعه پیشنهادات پیشگیرانه‌ای را برای تقویت پروتکل‌های امنیت داده‌ای سازمان‌ها ارائه می‌دهد تا از نفوذهای

	سیستم امنیتی محیطی	سیستم شناسایی نفوذ برنامه وب	
سیستم جلوگیری نفوذ برای شبکه	سیستم جلوگیری نفوذ برای برنامه وب	سیستم جلوگیری نفوذ برای رایانش ابری	سیستم شناسایی نفوذ برای شبکه ها
سیستم شناسایی نفوذ برای رایانش ابری	سیستم های حیاتی و زیرساخت عمومی	کنترل دسترسی کاربر	سیستم شناسایی نفوذ برای مرکز داده
	ضد بدافزار	سیستم جلوگیری نفوذ برای مرکز داده	

شکل ۲: معماری برنامه‌ای

پتانسیلی جلوگیری کنند. یکی از پیشنهادهای اصلی این است که نظارت امنیتی پیشگیرانه بالاتری اتخاذ شود. که شامل استفاده از ابزارها و سیستم‌ها برای نظارت پیوسته بر فعالیت‌های شبکه، شناسایی الگوهای غیرطبیعی و واکنش سریع به تهدیدات پتانسیلی در صورت رخداد شناسایی می‌شود. علاوه بر این، یک سیستم شناسایی نفوذ راهکاری حیاتی است تا سازمان‌ها بتوانند به صورت پیشگیرانه تهدیدات را شناسایی و مهار کنند قبل از اینکه بتوانند سیستم‌های آن‌ها را آسیب بزنند. با اجرای استراتژی‌های پیشگیرانه، سازمان‌ها می‌توانند آسیب‌پذیری خود در برابر تهدیدات سایبری را کاهش دهند. به جز شناسایی سریع تهدیدات، فرصتی برای اجرای تدابیر پیشگیرانه قبل از اینکه تأثیرات قابل توجهی بیفتد وجود دارد. بنابراین، این مطالعه بر اهمیت اجرای تدابیر پیشگیرانه برای حفاظت از داده‌های سازمانی و مدیریت مؤثر واکنش به تهدیدات سایبری تأکید می‌کند.

معماری برنامه‌ای سیستم‌های شناسایی نفوذ به طور قابل توجهی به حفاظت در برابر یک طیف گسترده از تهدیدات سایبری، به خصوص در شبکه‌های سازمانی، کمک می‌کند و این موضوع را به عنوان یک عنصر اساسی در اطمینان از امنیت معرفی می‌کند. درون یک شبکه سازمانی، سیستم شناسایی نفوذ به عنوان یک نگهبان مراقب و دقیق عمل می‌کند که به طور پیوسته جریان ترافیک شبکه را از منابع داخلی و خارجی نظارت می‌کند. هدف اصلی این سیستم، شناسایی خطرات پتانسیلی یا اقدامات مشکوک مانند حملات فیشینگ و نفوذهای آلوده به بدافزار است. این سیستم به عنوان یک سیستم هشدار دهنده پیشگیرانه، از طریق بررسی دقیق جریان شبکه عمل می‌کند و مدیران را از هرگونه نقضی که ممکن است به اهداف بدیهی و یا مخاطراتی در امنیت منجر شود، آگاه می‌سازد و اقدامات لازم را برای محافظت از سیستم‌ها و اطلاعات اتخاذ می‌کند. علاوه بر این، ادغام سیستم‌های شناسایی نفوذ به چارچوب امنیتی محیطی از جمله دیواره‌های آتشین و دروازه‌ها، قابلیت‌های دفاعی شبکه را بهبود می‌بخشد. در موقعیت‌های استراتژیکی در این نقاط بحرانی، سیستم‌های شناسایی نفوذ به طور دقیق و جدی جریان ترافیک شبکه ورودی و خروجی را نظارت می‌کنند. از این دیدگاه، سیستم‌های شناسایی نفوذ به طور مؤثر قادر به بررسی جریان‌های داده هستند، به سرعت حملات خارجی یا نقض امنیتی که به طور خاص به هدف انتقادی سازمان می‌پردازند را شناسایی و پیشگیری می‌کنند. این وظیفه اولیه این سیستم، تقویت از مرزهای خود و حفظ از نقاط ورودی احتمالی

از سوی دیگران است. همچنین، ادغام سیستم‌های شناسایی نفوذ در مراکز داده نقش حیاتی در بهبود وضعیت امنیتی زیرساخت‌های کلیدی سرور را بازی می‌کند. در این شرایط فعلی، سیستم‌های شناسایی نفوذ مسئولیت مداوم نظارت و حفاظت از سرورها و اجزای زیرساختی اساسی را بر عهده دارند. این سیستم با دقت جریان ترافیک شبکه را بررسی می‌کند و به سرعت خطرات ممکن مانند حملات انکار سرویس توزیع شده یا آزمایش‌های نفوذ را شناسایی کرده و به کار می‌برد. این از اهمیت بسیاری برای تضمین صحت و دسترسی به داده‌ها و سیستم‌های حیاتی است.

سیستم شناسایی نفوذ نقش کلیدی را در اطمینان از امنیت داده‌ها و برنامه‌هایی که در محیط‌های محاسبات ابری میزبانی می‌شوند، ایفا می‌کند. سیستم شناسایی نفوذ می‌تواند با بررسی ترافیکی که از زیرساخت ابری عبور می‌کند، تهدیدات سایبری را که برای خدمات ابری منحصر به فرد هستند شناسایی و با آن مقابله کند. این سیستم نقش حیاتی از محافظت در برابر خطرات ممکن را دارد که با استفاده از منابع مشترک و محیط‌های مجازی شکل می‌گیرند. علاوه بر این، سیستم‌های شناسایی نفوذ نقش اساسی در حفاظت از سیستم‌های حیاتی و زیرساخت‌های عمومی ایفا می‌کنند. این سیستم ها حفاظت و تقویت سیستم‌های زیرساختی اساسی را که برای ارائه خدمات عمومی ضروری هستند، محقق می سازد. سیستم شناسایی نفوذ در انواع صنایع از جمله انرژی، حمل و نقل و بهداشت استفاده می‌شود. این سیستم به عنوان یک مکانیزم نظارت جامع عمل کرده و به طور پیوسته تهدیدات ممکن را که قادر به مخلوط کردن خدمات اساسی هستند، نظارت و شناسایی می‌کند. هدف اصلی آن حفظ عملکرد بی‌وقفه این خدمات و حفاظت از رفاه عمومی است. در گسترده‌ترین کاربردها، سیستم‌های شناسایی نفوذ به عنوان یک موجود نظارتی عمل می‌کنند که روش‌ها و تکنیک‌های شناسایی خود را برای تطبیق با محیط‌های مختلف تغییر می‌دهند. ماهیت چندوجهی این فناوری آن را در حوزه‌های مختلف نظارت بر دسترسی کاربر، حفاظت از برنامه‌های وب، اطمینان از امنیت دستگاه‌های اینترنت اشیا، تجزیه و تحلیل رفتارهای مالوری و بهبود روش‌های آزمایش امنیتی، اساسی می‌کند. اهمیت سیستم‌های شناسایی نفوذ در تقویت شبکه‌ها و سیستم‌های معاصر در برابر حوزه پیوسته تغییرات تهدیدات سایبری، توسط این رویکرد جامع تاکید می‌شود.

۲.۳ معماری زیرساخت

معماری زیرساخت که با هدف امنیت برای سازمان‌ها آماده می‌شود، یک پایه اساسی برای اطمینان از حفاظت و قابلیت اعتماد سیستم‌ها و داده‌هایی است که آن‌ها در اختیار دارند. این معماری شامل یک سری لایه‌های پیوندی است که به همراه کار می‌کنند تا از سازمان‌ها در برابر تهدیدات سایبری متنوع و در حال تکامل محافظت کنند. اولین لایه، لایه سرور، مرکز اصلی این زیرساخت است. در این لایه، سرورهایی که برنامه‌ها را اجرا می‌کنند و داده‌های سازمان را ذخیره می‌کنند قرار دارند. امنیت در این لایه برای حفاظت از دسترسی به اطلاعات حساس حیاتی است و این کار از طریق تنظیمات دسترسی مناسب، رمزگذاری داده‌ها و نظارت مداوم بر فعالیت‌های مشکوک انجام می‌شود. لایه شبکه به عنوان استخوانه پیوندی عمل می‌کند. انواع سیستم‌ها و دستگاه‌ها در شبکه سازمان قرار دارند. دستگاه‌هایی مانند روترها، سوئیچ‌ها و سایر زیرساخت‌های شبکه در این لایه قرار دارند. امنیت در این لایه اساسی است زیرا این مسیر برای حرکت داده بین انواع دستگاه‌ها

شکل ۳: معماری زیرساخت

استفاده می‌شود. رمزگذاری داده، کنترل دسترسی و نظارت بر ترافیک شبکه اهمیت زیادی برای حفظ امنیت این لایه دارند.

دیوار آتشین و سیستم های تشخیص و جلوگیری از نفوذ (چادویک و همکاران، ۲۰۲۰؛ مانتا و همکاران، ۲۰۲۱)، لایه های اصلی در دفاع سازمان در برابر حملات خارجی هستند. فایروال مسئول بررسی و مدیریت ترافیک ورودی و خروجی شبکه است، در حالی که سیستم های تشخیص و جلوگیری از نفوذ به طور فعال فعالیت شبکه را نظارت می‌کند تا الگوها یا نشانه‌های مشکوک به تهدیدات را شناسایی کند. هر دوی این نقش‌ها اساسی در مقابله با حملات و تنش‌های امنیتی دارند و پاسخ‌های سریعی به تهدیدات شناسایی شده ارائه می‌دهند. در نهایت، لایه امنیت برنامه کاربردی برای حفاظت از برنامه‌های استفاده شده توسط سازمان بسیار حیاتی است. این شامل اقدامات امنیتی مانند رمزگذاری داده‌ها، مدیریت دسترسی دقیق، و پیاده‌سازی شیوه‌های امنیتی در توسعه و نگهداری برنامه است. این لایه به دلیل اینکه برنامه‌ها معمولاً هدف آسان حملات سایبری هستند، حیاتی است. با توجه به این چهار لایه، سازمان‌ها می‌توانند پایه اساسی و جامعی از امنیت را ایجاد کنند. ترکیب هر یک از این لایه‌ها دفاع جامعی را فراهم می‌کند، اطمینان حاصل می‌شود که سیستم‌ها و داده‌های سازمان از تهدیدات مختلف سایبری که ممکن است به عملکرد و پیوستگی عملیاتی سازمان خسارت وارد کنند، به‌طور مؤثری محافظت می‌شوند.

تصویر ۳ نمایش‌دهنده‌ی معماری زیرساخت است که به عنوان پایه‌ای اساسی برای تضمین امنیت سیستم اطلاعاتی عمل می‌کند. این طراحی معماری به چهار لایه متمایز تقسیم شده است که چارچوبی انعطاف‌پذیر برای حفاظت و نظارت بر منابع دیجیتال سازمان فراهم می‌آورد. لایه اول، که به عنوان لایه سرور شناخته می‌شود، به عنوان مؤلفه‌ی اصلی این زیرساخت عمل می‌کند. در این سیستم، یک مجموعه از سرورها وجود دارد که مسئول ارائه خدمات و برنامه‌های لازم بر اساس درخواست‌های سازمان هستند. این شامل سرورهای برنامه، پایگاه‌داده‌ها و مجموعه‌ای از سرویس‌های دیگر می‌شود. اهمیت امنیت در این لایه نباید نادیده گرفته شود، زیرا سرور به عنوان دروازه‌ی اصلی برای کاربران داخلی و خارجی عمل می‌کند. برای تضمین پایداری

و قابلیت اعتماد سیستم، مدیریت دسترسی، امنیت فیزیکی، و نظارت بر سلامت سرور اولویت دارد.

لایه بعدی، لایه شبکه، به عنوان زیرساخت اصلی برای فراهم‌آوردن ارتباطات میان انواع مختلف سیستم‌ها عمل می‌کند. این لایه شامل دستگاه‌های شبکه مانند روترها، سوییچ‌ها و سایر دستگاه‌هاست که نقل و انتقال داده را در داخل شبکه کنترل می‌کنند. اطمینان از امنیت در این لایه از اهمیت بالایی برخوردار است برای حفظ صحت و محرمانگی داده‌ها در طول انتقال آنها در نقاط مختلف شبکه. پیاده‌سازی رمزنگاری داده، نظارت بر ترافیک و پیکربندی‌های مناسب دسترسی شبکه می‌تواند به طور مؤثر این حفاظت را تضمین کند. لایه بعدی مربوط به لایه دیوار آتش / سیستم تشخیص نفوذ است که مسئولیت حفاظت از امنیت محیطی را بر عهده دارد. یک دیوار آتش به عنوان خط دفاع اولیه عمل می‌کند که جریان ترافیک داده را در ورود و خروج از شبکه بررسی و کنترل می‌کند. در همین حال، یک سیستم تشخیص نفوذ به منظور نظارت فعال بر فعالیت شبکه استفاده می‌شود با هدف شناسایی و نشان دادن الگوها یا رفتارهای غیرعادی که ممکن است به حمله اشاره داشته باشند یا تهدیدی برای سیستم باشند (وارگا و همکاران، ۲۰۲۱). همکاری بین این دو نهاد به منظور کاهش دسترسی غیرمجاز و شناسایی و حل مشکل تهدیدات سایبری موجود می‌باشد.

لایه امنیت برنامه‌ها به عنوان حفاظت اصلی در برابر تهدیدات داخلی و خارجی که ممکن است باعث تخلیه و امنیت برنامه‌های استفاده شده در سازمان شود، عمل می‌کند. این لایه شامل مجموعه‌ای از فناوری‌های امنیتی است که شامل رمزنگاری داده، مدیریت دسترسی کاربر و پیاده‌سازی شیوه‌های امنیتی در کد برنامه برای کاهش حملات ممکن مانند حقه‌زنی SQL یا اسکریپت نویسی از جا به جایی[۶] است. از آنجا که افراد بدجنس به طور مکرر برنامه‌ها را هدف قرار می‌دهند، اجرای اقدامات قوی امنیتی در این سطح بسیار حیاتی است. با تمرکز دقیق بر این چهار لایه، سازمان‌ها می‌توانند یک چارچوب امنیتی قدرتمند در زیرساخت خود ایجاد کنند. ادغام این چهار لایه به مدیران فناوری اطلاعات امکان می‌دهد تا به طور مؤثر به دستگاه امنیتی جامعی راه‌اندازی کنند، احتمال تهدیدات سایبری را کاهش دهند و اطمینان حاصل کنند که حفاظت از محرمانگی و صحت داده‌ها و سیستم‌های اطلاعاتی سازمان تضمین شده است.

۴ بحث

بررسی اهمیت معماری سازمانی در کاهش خطرات تجاری و تهدیدات سایبری نشان می‌دهد که ادبیات علمی گسترده‌ای در این زمینه وجود دارد که تأکید می‌کند به تأثیر بحرانی آن. اهمیت این موضوع به عنوان یک مانع پیشگیرانه در برابر تهدیدات سایبری پیوسته‌تغییر، هم‌آهنگ با اهداف استراتژیک کسب‌وکارها، در مطالعات متعدد برجسته شده است. این پرس و جو رویکردهای استفاده شده توسط معماری سازمانی را برای تقویت تاب‌آوری سایبری مورد بررسی قرار می‌دهد، و اجرای آن با استراتژی‌های مدیریت خطر برای اطمینان از حفاظت در برابر خطرات محتمل و طیف گسترده‌ای از تهدیدات را پیگیری می‌کند. بررسی بعدی به بررسی آگاهی از تهدید سایبری (CTI)[۷] می‌پردازد که در حمایت از سازمان‌ها بسیار مهم است، اما نرخ پذیرش آن

[6] Cross-Site Scripting
[7] Cyber-Threat Intelligence (CTI)

پایین است. ادبیات مربوط به آگاهی از تهدید سایبری به طور قابل توجهی تحت تأثیر فناوری قرار دارد و باعث ایجاد شکاف‌های دانشی می‌شود. این مطالعه پایه‌های نظری، روش‌های تحقیق عملی، و نقش اشیاء و سیستم‌های اطلاعاتی در اجرای آگاهی از تهدید سایبری را بررسی می‌کند (اینسلای و همکاران، ۲۰۲۳). این مقاله یک روش‌شناسی معرفی می‌کند که برای شبکه‌های هوشمند، ادغام ارزیابی خطر و مدل‌سازی تهدید را مدیریت می‌کند. هدف از این کار توسعه مجموعه جامعی از نیازهای امنیتی برای ادغام انرژی‌های تجدیدپذیر در معماری شبکه ولتاژ پایین است (مارکشتینر و همکاران، ۲۰۱۹). این مقاله تأسیس یک چارچوب مدل‌سازی تهدید برای سیستم‌های هوشمند فیزیکی-سایبری (CPS)[۸] را پیشنهاد می‌دهد تا خطرات امنیتی پتانسیلی را شناسایی کند. از ماتریس MITRE ATT&CK و مجموعه نیازهای سیستم برای تولید یک لیست تهدید برای یک سیستم آتش‌نشانی هوشمند استفاده می‌شود، که نشان دهنده پتانسیل حفاظت و کاهش تهدیدات آن است (زاهید و همکاران، ۲۰۲۳). این مطالعه بررسی خطرات امنیتی و چالش‌های فنی تکنولوژی Ag-IoT را انجام می‌دهد، با تمرکز بر برنامه‌های جدید ظاهرشده، معماری‌ها، حملات مشکوک و چالش‌ها در پاسخ به وقایع و کرایه‌های دیجیتال. این مقاله به این نتیجه می‌رسد که اطمینان از امنیت بسیار مهم است برای ارائه خدمات و محقق شدن مؤثر در بخش کشاورزی هوشمند (رودراکار و روغنی، ۲۰۲۳). حملات سایبری تأثیر گذار بر زندگی ما است، که نیاز به همکاری برای ایمنی سایبری دارد. یک مدل اعتماد پنج سطحی برای زیرساخت اشتراک داده‌های ابر-لبه به خصوصیت در مورد اشتراک سری تجهیزات. مدل آگاهی از تهدید سایبری به مالکان داده‌ها امکان می‌دهد که سطح اعتماد و رویه‌های بهداشتی را انتخاب کنند، که پیاده‌سازی و آزمایش توسط چهار پروژه آزمایشی انجام شده است (چادویک و همکاران، ۲۰۲۰). CAESAR8 یک رویکرد نوآورانه است که به پیاده‌سازی ارزیابی‌های پویا و جامع مرتبط با خطرات امنیت اطلاعات در پروژه‌های فناوری اطلاعات تأکید می‌کند. این ارزیابی از رشد و امنیت در هشت حوزه، مشکلات واقعی را بررسی می‌کند، به خصوص برای سازمان‌های کوچک (لافت و همکاران، ۲۰۲۲).

چه روش‌ها و عوامل حیاتی بهینه در ادغام معماری سازمانی برای مدیریت جامع امنیت سایبری وجود دارند؟ ادغام معماری سازمانی برای مدیریت جامع امنیت سایبری شامل مجموعه‌ای از روش‌های سازمان‌یافته است که چالش‌های پیچیده در حوزه امنیت دیجیتال را حل می‌کند. روش‌های بهینه و عوامل حیاتی این رویکردها را هدایت می‌کنند. رویکرد مبتنی بر خطر به عنوان یک روش مؤثر شناخته می‌شود که با شناسایی خطرات پتانسیلی، اولین مرحله در تدوین یک استراتژی امنیتی مناسب است. معماری سازمانی به عنوان یک روش برای بررسی و تعریف زیرساخت‌های آسیب‌پذیر، فرآیندهای تجاری و دارایی‌های ارزشمند عمل می‌کند و سپس اقدامات امنیتی مناسب را برای کاهش این خطرات مشخص می‌کند. یک رویکرد دیگر شامل بهره‌گیری از استانداردها و چارچوب‌های تطابق است. ادغام معماری سازمانی در حوزه امنیت سایبری به معنای تطبیق با استانداردها و چارچوب‌های جهانی شناخته شده مانند ISO/IEC ۲۷۰۰۱، چارچوب امنیت سایبری NIST یا COBIT است. پیاده‌سازی معماری سازمانی بر اساس این استانداردها امری حیاتی است که تضمین می‌کند سیستم‌های امنیتی مطابق با نیازهای تنظیمی باشند و قادر به مقابله با انواع مختلف

[8] Cyber-Physical System (CPS)

تهدیدات سایبری باشند.

ایجاد یک معماری امنیتی یکپارچه از اهمیت بسیاری برخوردار است. این شامل توسعه یک طراحی سیستم جامع است که همچنین شامل سطح زیرساخت و برنامه‌های خاص می‌شود. حوزه معماری سازمانی در زمینه عملیات سازمانی اهمیت زیادی دارد. تجزیه و تحلیل جامع و ادغام اقدامات امنیتی در تمام سطوح چارچوب معماری از این قرار است که شامل شناسایی نقاط ضعف و سپس شناسایی و پیاده‌سازی استراتژی‌های مناسب برای تقویت مکانیسم‌های دفاعی موجود می‌شود. به علاوه، درگیری سایر ذینفعان، عامل مذکور نقش حیاتی را در تایید نتیجه ایفا می‌کند شامل چندین بخش یا واحد کسب و کار در برنامه‌ریزی و اجرای معماری سازمانی ضروری است. ارتباط مؤثر میان تیم‌های امنیتی، توسعه‌دهندگان، مدیران کسب و کار و سایر ذینفعان و برای ادغام موفق معماری سازمانی در مدیریت جامع امنیت سایبری بسیار حیاتی است. نظارت و ارزیابی مداوم همچنین جزء ضروری است. پس از پیاده‌سازی یک معماری سازمانی، حائز اهمیت است که به طور مداوم کارآیی آن در کاهش تهدیدات سایبری ظاهر شده را نظارت و ارزیابی کنیم. طبیعت پویای پیشرفت‌های فناوری و پراکندگی تهدیدات سایبری نیازمند به‌روزرسانی و سازگاری مداوم معماری سازمانی برای پاسخ به نیازهای نوظهور هستند. با استفاده از روش‌های مناسب مانند رویکرد مبتنی بر خطر و استانداردها، و با توجه به ادغام معماری امنیتی، درگیری ذینفعان و ارزیابی مداوم، ادغام معماری سازمانی می‌تواند به عنوان پایه‌ای قوی برای مدیریت جامع و قابل تطبیق امنیت سایبری عمل کند که با پویایی‌های مداوم تهدیدات سایبری همگام است.

تأثیر هم‌آمیختن معماری سازمانی با اهداف تجاری در افزایش تاب‌آوری در برابر تهدیدات سایبری نوظهور چیست؟ هم‌آمیختن معماری سازمانی با اهداف تجاری تأثیر قابل توجهی بر افزایش تاب‌آوری در برابر تهدیدات سایبری نوظهور دارد. زمانی که معماری سازمانی به طور استراتژیک با اهداف تجاری سازمان‌ها باهم‌آمیخته می‌شود، این امر باعث می‌شود که آنها بتوانند به شیوه جامع و پیش‌بینانه‌ای به تغییرات مداوم منظره تهدیدات سایبری پاسخ دهند. یکی از اثرات آن، درک بهتری از خطرات مرتبط با هر پیش‌کاری تجاری انجام شده است. معماری سازمانی نقش حیاتی در شناسایی نقاط ضعف در زیرساخت‌ها و فرآیندهای تجاری دارد که ممکن است در برابر حملات حساس باشند. این باعث می‌شود که استراتژی‌های امنیتی جامع و متمرکزی تدوین شود.

به علاوه، هم‌آمیختگی بین معماری سازمانی و اهداف تجاری، فرآیندهای تصمیم‌گیری مستندتر در مدیریت سرمایه‌گذاری‌های فناوری را تسهیل می‌کند. معماری سازمانی نقش حیاتی در درک این مورد دارد که چگونه یک فناوری خاص در دستیابی به اهداف تجاری کمک می‌کند. این درک به سازمان‌ها قدرت می‌دهد تا در تصمیم‌گیری‌های مبنی بر سرمایه‌گذاری‌ها، مستندتر و استراتژیک‌تر عمل کنند. این رویکرد امکان بهینه‌سازی استفاده از منابع را فراهم می‌کند و به کارایی مدیریتی افزوده می‌کند، با تأکید بر ادغام بی‌درنگ در نظر گرفتن ملاحظات امنیتی در مراحل اولیه توسعه یا پیاده‌سازی فناوری.

هنگامی که الکترونیک آرتز با اهداف تجاری خوب تعریف شده هم‌آمیخته می‌شود، فرآیندهای تصمیم‌گیری شتاب‌زده را تسهیل می‌کند و به طور مؤثر با تهدیدات نوظهور سازگار می‌شود. در زمینه منظره

دینامیک و در حال تحول کسب‌وکار، هم‌گام‌سازی اهداف سازمانی و استراتژی‌های امنیتی توانایی سازگاری و چابکی بیشتر را فراهم می‌کند. پیاده‌سازی یک معماری سازمانی یکپارچه، توسعه زیرساخت قوی را که قادر به به‌سرعت تنظیم به شرایط پویا است، تسهیل می‌کند و این باعث افزایش سرعت و کارایی در مقابله با تهدیدات سایبری نوظهور می‌شود. علاوه بر این، هم‌آمیختگی بین معماری سازمانی و اهداف تجاری به بهبود آگاهی کلی از امنیت سایبری در سازمان کمک می‌کند. این اقدام به ارتقای فرهنگ سازمانی سازمان با ترویج یک رویکرد فعال در مقابله با تهدیدات سایبری کمک می‌کند. این تلاش به افزایش آگاهی و ایجاد یک حس توجه بیشتر در میان همه اعضای سازمان در خصوص اتخاذ شیوه‌های امنیتی قوی می‌پردازد. این امر موجب بهبود استراتژی دفاعی جامع سازمان می‌شود، زیرا هر عضو در سازمان به طور فعال در تلاش برای حفظ تدابیر امنیتی سازمان تلاش می‌کند.

بطور کلی، هم‌آمیختگی معماری سازمانی با اهداف تجاری به عنوان پایه‌ای قوی برای افزایش تاب‌آوری سازمان در برابر تهدیدات سایبری پویا عمل می‌کند. این ادغام با فراهم آوردن درک بهتری از خطرات، تخصیص استراتژیک‌تر سرمایه‌گذاری‌های فناوری، پاسخ سریع‌تر به تهدیدات نوظهور، و تربیت فرهنگ امنیتی تقویت شده، به سازمان‌ها کمک می‌کند تا چارچوب‌های مقاومی برای مدیریت مؤثر منظره امنیتی پویای دوران دیجیتال معاصر بسازند.

۵ نتیجه‌گیری

دوران دیجیتال چالش‌های منحصر به فردی را برای کسب‌وکارها به دلیل پیشرفت‌های فناورانه و چشم‌انداز گسترده تهدیدات سایبری ارائه می‌دهد. معماری سازمانی به عنوان پایه‌ای برای ساخت سیستم‌های اطلاعاتی سازمانی برای تقویت دفاع و مدیریت خطرات تجاری تبدیل شده است. مکانیسم‌های دفاع سنتی نسبت به حملات سایبری مانند نفوذ به داده‌ها، حملات رنسومر، و تخریب سیستم، آسیب‌پذیر هستند. این مطالعه به بررسی کارآمدی معماری سازمانی در برخورد با تهدیدات امنیت سایبری و مدیریت خطرات تجاری مرتبط می‌پردازد. سیستم پیشگیری و شناسایی نفوذ، یک مؤلفه حیاتی در امنیت سایبری است که برای شناسایی، مهار، و پاسخ به تهدیدات سایبری طراحی شده است. چارچوب معماری گروه باز، یک رویکرد ساختارمند برای توسعه معماری سازمانی است که شامل جنبه‌های تجاری و فناوری می‌شود. سیستم‌های پیشگیری و شناسایی نفوذ برای محافظت در برابر انواع تهدیدات سایبری، به خصوص در شبکه‌های سازمانی، ضروری هستند. معماری زیرساخت، که به چهار لایه تقسیم شده است، یک چارچوب مقاوم برای حفاظت از منابع دیجیتال یک سازمان فراهم می‌کند. تعدادی پیشنهاد عملی برای سازمان‌ها برای اجرای اقدامات زیر عبارتند از:

۱. انجام ارزیابی‌های امنیتی روزانه: این شامل انجام بازرسی‌های امنیتی دوره‌ای برای شناسایی ضعف‌ها یا شکاف‌های سیستم است. با انجام نظارت و ارزیابی مداوم، سازمان‌ها می‌توانند پیاده‌سازی تدابیر پیشگیری یا تصحیح را به سرعت تسریع دهند.

۲. به‌روزرسانی نرم‌افزارها و سیستم‌عامل: اطمینان از به‌روزرسانی منظم نرم‌افزارها و سیستم‌عامل‌های استفاده شده توسط سازمان از اهمیت بالایی برخوردار است. به‌طور مکرر، این به‌روزرسانی‌ها شامل چسبانده‌های امنیتی هستند که به تقویت سیستم در برابر تهدیدات جدید کمک می‌کنند.

۳. آموزش کارکنان درباره امنیت اطلاعات: ضروری است که به کارکنان آموزش مداوم درباره روش‌های امنیت اطلاعات داده شود. افراد باید از خطرات پتانسیلی آگاه باشند و قابلیت شناسایی و گزارش دادن در مواقع مشکوک را داشته باشند.

۴. پیاده‌سازی سیستم شناسایی و جلوگیری از نفوذ: ایجاد یک سیستم شناسایی و جلوگیری از نفوذ پیچیده و کارآمد به سازمان‌ها اجازه می‌دهد که به سرعت فعالیت‌های مشکوک را شناسایی و برطرف کنند، و از فرماندهی سیستم جلوگیری کنند.

۵. توسعه طرح پاسخ به حوادث: سازمان باید یک طرح جامع پاسخ به حوادث تعریف کند. این طرح شامل روش‌هایی برای برخورد با حملات سایبری یا نقض امنیتی، از جمله بازیابی داده‌ها و سیستم است.

۶. نظارت و تجزیه و تحلیل روندهای امنیتی: نظارت و تحلیل روندهای امنیتی می‌تواند در پیش‌بینی تهدیدات آینده کمک کند. این امر به سازمان‌ها اجازه می‌دهد که به صورت پیشگیرانه از خطرات مرتبط با تهدیدات مورد انتظار مقابله کنند.

این مطالعه نقاط ضعف پیشنهاد خود را که بر توجه به پیاده‌سازی زیرساخت و برنامه‌ها برای امنیت سایبری تمرکز دارد، آشکار می‌سازد. نیاز به تحقیقات بیشتری وجود دارد تا به پیاده‌سازی‌های پیچیده‌تر و جامع‌تر و با تأکید خاص بر برنامه‌ها و زیرساخت‌های امنیتی در شبکه‌های فناوری اطلاعات سازمانی بپردازد.

این بسیار حیاتی است که به بررسی عمیق‌تر پیاده‌سازی پرداخته شود. این شامل روش‌های جامع برای ادغام برنامه‌های امنیت سایبری به زیرساخت فناوری اطلاعات یک سازمان می‌شود، که شامل سیستم‌های تشخیص نفوذ، رمزنگاری داده‌ها و مدیریت هویت است. علاوه بر این، تأکید بر زیرساخت نیازمند بررسی جامع‌تری است که شامل طراحی، پیکربندی و مدیریت شبکه می‌شود، که باید به طور مؤثر لایه‌های امنیتی را یکپارچه کند. تحقیقات بیشتر در این حوزه ممکن است مطالعات موردی را که شامل پیاده‌سازی عملی در گستره‌ای از سناریوهای کسب و کار هستند، مورد بررسی قرار دهد. این به فهم مشکلات پتانسیلی که در طول فاز پیاده‌سازی ممکن است پدید آید، همراه با ابداع راه‌حل‌های مؤثر برای حل این مشکلات، کمک می‌کند. همچنین، بسیار مهم است که جنبه‌های مدیریت خطر مربوط به پیاده‌سازی اقدامات امنیتی مورد توضیح قرار گیرد. با اولویت‌دهی به ارزیابی خطر، فرمولاسیون سیاست‌های امنیتی و ارزیابی عملکرد پس از پیاده‌سازی سیستم‌های امنیتی، می‌توان به درک جامع‌تری از کارایی اقدامات انجام شده دست یافت. تحقیقات بیشتر در این حوزه ممکن است به درک جامع‌تر و قابل استفاده‌تری از اینکه چگونه پیاده‌سازی زیرساخت و امنیت سایبری می‌تواند در محیط‌های شبکه فناوری اطلاعات سازمانی بهبود یابد، منجر شود.

مراجع

[1] Hindarto, D., Indrajit, R.E. and Dazki, E., 2021. Sustainability of Implementing Enterprise Architecture in the Solar Power Generation Manufacturing Industry. Sinkron: jurnal dan penelitian teknik informatika, 6(1), 13- 24. https://doi.org/10.33395/sinkron.v6i1.11115

[2] Amanda, D., Hindarto, D., Indrajit, E. and Dazki, E., 2023. Proposed use of TOGAF-Based Enterprise Architecture in Drinking Water Companies. Sinkron: jurnal dan penelitian teknik informatika, 8(3), 1265-1277. https://doi.org/10.33395/sinkron.v8i3.12477

[3] Iswahyudi, I., Hindarto, D. and Indrajit, R.E., 2023. Digital Transformation in University: Enterprise Architecture and Blockchain Technology. Sinkron: jurnal dan penelitian teknik informatika, 8(4), 2501-2512. https://doi.org/10.33395/sinkron.v8i4.12977

[4] Hindarto, D., 2023. Blockchain-Based Academic Identity and Transcript Management in University Enterprise Architecture. Sinkron: jurnal dan penelitian teknik informatika, 8(4), 2547-2559. https://doi.org/10.33395/sinkron.v8i4.12978.

[5] Hindarto, D. and Santoso, H., 2021. Android APK Identification using Non Neural Network and Neural Network Classifier. Journal of Computer Science and Informatics Engineering, 5(2), 149-157. https://doi.org/10.29303/jcosine.v5i2.420

[6] Hindarto, D. and Santoso, H., 2022. Performance Comparison of Supervised Learning Using Non-Neural Network and Neural Network. Jurnal Nasional Pendidikan Teknik Informatika: JANAPATI, 11(1), 49-62. https://doi.org/10.23887/janapati.v11i1.40768

[7] Sari, R.T.K. and Hindarto, D., 2023. Implementation of Cyber-Security Enterprise Architecture Food Industry in Society 5.0 Era. Sinkron: jurnal dan penelitian teknik informatika, 8(2), 1074-1084. https://doi.org/10.33395/sinkron.v8i2.12377

[8] Hasan, M.K., Habib, A.A., Shukur, Z., Ibrahim, F., Islam, S. and Razzaque, M.A., 2023. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. Journal of Network and Computer Applications, 209, 103540. https://doi.org/10.1016/j.jnca.2022.103540

[9] Chadwick, D.W., Fan, W., Costantino, G., De Lemos, R., Di Cerbo, F., Herwono, I., Manea, M., Mori, P., Sajjad, A. and Wang, X.S., 2020. A cloud-edge based data security architecture for sharing and analysing cyber threat information. Future generation computer systems, 102, 710-722. https://doi.org/10.1016/j.future.2019.06.026

[10] Mantha, B., de Soto, B.G. and Karri, R., 2021. Cyber security threat modeling in the AEC industry: An example for the commissioning of the built environment. Sustainable Cities and Society, 66, 102682. https://doi.org/10.1016/j.scs.2020.102682

[11] Varga, S., Brynielsson, J. and Franke, U., 2021. Cyber-threat perception and risk management in the Swedish financial sector. Computers & security, 105, 102239. https://doi.org/10.1016/j.cose.2021.102239

[12] Ainslie, S., Thompson, D., Maynard, S. and Ahmad, A., 2023. Cyber-Threat Intelligence for Security Decision-Making: A Review and Research Agenda for Practice. Computers & Security, 103352. https://doi.org/10.1016/j.cose.2023.103352

[13] Marksteiner, S., Vallant, H. and Nahrgang, K., 2019. Cyber security requirements engineering for low-voltage distribution smart grid architectures using threat modeling. Journal of Information Security and Applications, 49, 102389. https://doi.org/10.1016/j.jisa.2019.102389

[14] Zahid, S., Mazhar, M.S., Abbas, S.G., Hanif, Z., Hina, S. and Shah, G.A., 2023. Threat modeling in smart firefighting systems: Aligning MITRE ATT&CK matrix and NIST security controls. Internet of Things, 22, 100766. https://doi.org/10.1016/j.iot.2023.100766

[15] Rudrakar, S. and Rughani, P., 2023. IoT based agriculture (Ag-IoT): A detailed study on architecture, security and forensics. Information Processing in Agriculture. https://doi.org/10.1016/j.inpa.2023.09.002

[16] Loft, P., He, Y., Yevseyeva, I. and Wagner, I., 2022. CAESAR8: An agile enterprise architecture approach to managing information security risks. Computers & Security, 122, 102877. https://doi.org/10.1016/j.cose.2022.102877.