امنیت محیطی در حوزه
فناوری اطلاعات و ارتباطات

فهرست

آغاز

طبق نظریه سامانه‌ها، هر سامانه دارای محیطی است که آن را فرا گرفته و با آن در تأثیر و تأثر است. هر سامانه به عنوان یک کل، بر محیط خود اثراتی دارد که ممکن است مثبت یا منفی و مفید یا مضر باشند. از سوی دیگر سامانه نیز از محیط تأثیر می‌پذیرد که این تأثیرات محیطی نیز ممکن است برای سامانه مفید یا مضر باشند. نکته‌ی دیگر در ارتباط بین سامانه و محیط این است که سامانه برای بقا نیازمند ورودی‌هایی است که این ورودی‌ها از محیط تأمین می‌گردند. به عنوان مثال انرژی، مواد اولیه، اطلاعات و مواردی از این قبیل ورودی‌هایی هستند که باید از محیط تأمین شوند.

از طرفی سامانه باید برای ورودی‌های خود دارای فرآیندهای کدینگ و فیلترینگ باشد. به عبارت دیگر هر سامانه ورودی‌های خود را بررسی کرده و در صورتی که مطابق روال موردنظر سامانه نباشد، آن‌ها را فیلتر می‌کند. اگر فرآیند فیلترینگ در سامانه به خوبی تعریف نشده باشد، امنیت، ایمنی و پایداری سامانه به مخاطره می‌افتد. فرآیندهای فیلترینگ با توجه به ادبیات امنیت در واقع شامل سیاست‌های امنیتی سامانه هستند و درست تعریف کردن این سیاست‌ها با توجه به شرایط محیط ضامن بقاء و پایداری سامانه خواهد بود. به عبارت دیگر اگر سامانه توانایی تشخیص ورودی‌های مفید و مضر از یکدیگر را نداشته باشد، ممکن است هدف تهدیدات متعددی قرار بگیرد.

باید در نظر داشت که می‌توان محیط را بستری تعریف کرد که سامانه در آن موجودیت می‌یابد. یا به عبارت بهتر، بدون تعیین مرز سامانه ، نمی‌توان برای آن هدف یا عملکردی را تعریف نمود.

با توجه به آن‌چه تا کنون گفته شد، امنیت محیطی یکی از اجزای ضروری و لاینفک سامانه است. از این رو نمی‌توان موضوع تدوین، ابلاغ و اجرای سیاست‌های امنیتی را از مدیریت سازمان جدا دانست. بنابراین مسؤولیت تأمین امنیت بر عهده همان فردی است که مدیریت سامانه را پذیرفته است. چراکه تدوین سیاست‌های کلی، راهبری و نظارت بر اجرای همین سیاست‌ها در همه‌ی بخش‌ها از جمله امنیت بر عهده‌ی مدیریت سامانه است. از سوی دیگر باید در نظر داشت که لازم است ملاحظات مربوط به امنیت، ایمنی و پایداری و همچنین رویه‌های نظارت بر آن در همه‌ی هدف‌گذاری‌ها و سیاست‌های سازمان منظور شود.

همان‌طور که پیش از این اشاره شد، با نگرش سامانهی به فناوری اطلاعات و ارتباطات، هر سامانه به عنوان یک کل دارای اجزای مختلفی است و محدوده و مرز مشخصی در تعامل با پیرامون خود دارد.

هر چند امنیت سامانه به امنیت اجزای آن وابسته است، باید توجه داشت که امنیت، یک بخش مجزا از سامانه نیست که محدوده مشخصی در سامانه داشته باشد.

در حوزه فناوری اطلاعات و ارتباطات نیز اغلب سامانه‌ها دارای بخش‌ها یا اجزای فیزیکی هستند. به عنوان مثال در یک سامانه تبادل اطلاعات در فضای سایبر، بخش‌های فیزیکی مختلفی شامل سرورها، ابزارهای ذخیره‌سازی اطلاعات و بستر شبکه‌ی ارتباطی وجود دارد. به عبارت دیگر علی‌رغم اینکه فضای سایبر برای بسیاری از کاربران مفهوم فضایی مجازی و غیرفیزیکی دارد، این فضا دارای پایه‌هایی فیزیکی است که اطلاعات، خدمات، پروتکل‌ها و سایر مفاهیم مجازی بر پایه آن بنا شده است. به همین دلیل است که برقراری امنیت فیزیکی و محیطی، پیش‌نیاز اصلی برقراری امنیت در سامانه‌های فناوری اطلاعات و ارتباطات، به شمار می‌آید. به عبارت

دیگر اگرچه اطلاعات موجود در فضای سایبر و یا سرویس‌هایی که سازمان‌ها با به‌کارگیری فناوری اطلاعات و ارتباطات برقرار نموده‌اند، اهمیتی کلیدی برای آن‌ها دارد، اما امنیت و استقرار هر جزء، حتی کوچک، از سخت‌افزار و فیزیک این تجهیزات به دلیل این‌که بستر برقراری این سرویس‌ها هستند اهمیت بالاتری دارد.

سازمان های مبتنی بر فناوری اطلاعات و ارتباطات برای ارتباط با محیط متغیر بیرون با تحولاتی رودررو می‌شوند و به منظور کاهش مخاطرات محیطی به ضوابط و سیاست‌های امنیت محیطی نیاز دارند. در امنیت محیطی نیز، هدف تأمین سه عامل امنیت، ایمنی و پایداری است. منظور از این موضوع، ایجاد روند ها و راهکارهایی برای عدم اثرگذاری مخرب عوامل خارجی بر سامانه اطلاعاتی و ارتباطی است.

هرچند ملاحظات امنیت فیزیکی تنها عواملی هستند که در ابتدای بررسی این حوزه به ذهن متبادر می‌شوند، اما برخی عوامل دیگر نیز فراتر از کنترل‌های امنیت فیزیکی در تأمین امنیت محیطی اثرگذار هستند. ملاحظات آمایش سرزمین نظیر پراکندگی، مقابله با حوادث طبیعی و محافظت در قبال شرایط اجتماعی و نیز ملاحظات پیرامونی از جمله این عوامل است. از طرفی استفاده از عوارض طبیعی و نیز داشتن سناریوهای پوششی برای مراکز حیاتی، حساس و مهم از جمله ابزارهای تأمین امنیت محیطی هستند.

دارایی‌های ارزشمند سازمان اعم از تجهیزات سخت‌افزاری، ساختمان، منابع انسانی، اطلاعات و دانش تولید شده در سازمان در معرض مخاطرات مختلفی قرار دارند. این مخاطرات که در ادبیات امنیت ریسک یا مخاطره نامیده می‌شود، عبارت است از احتمال وقوع و میزان آسیبی که در اثر تخریب یکی از دارایی‌های ارزشمند به سازمان وارد می‌شود. به عبارت دیگر در ریسک یک دارایی احتمال بروز یک تهدید و میزان آسیب‌پذیری دارایی از آن و همچنین میزان صدمه‌ای که سازمان از آسیب این دارایی می‌بیند مورد توجه قرار می‌گیرد. با توجه به این تعریف باید در نظر

داشت که در بررسی ملاحظات امنیتی، دو موضوع آسیب‌پذیری‌های درونی و هم‌چنین تهدیدهای بیرونی باید مورد بررسی قرار گیرند.

امنیت فیزیکی

به منظور تأمین امنیت فیزیکی و محیطی فناوری اطلاعات و ارتباطات در سازمان‌ها و مراکز حیاتی، حساس و مهم باید به هر سه جنبه‌ی دفاع غیرعامل که شامل امنیت، ایمنی و پایداری است، توجه کرد. یکی از دیدگاه‌های مطرح در بحث‌های پدافند غیرعامل، امنیت فیزیکی و محیطی را تنها در حوزه ایمنی در نظر می‌گیرد. اما باید توجه داشت که در حوزه‌ی فناوری اطلاعات و ارتباطات بحث‌های مربوط به پایداری و امنیت نیز باید مد نظر قرار گیرند. زیرا در سازمان‌هایی که از خدمات فناوری اطلاعات و ارتباطات استفاده می‌کنند، ایجاد اختلال در دو رکن امنیت و پایداری هم می‌تواند منجر به خدشه‌دار شدن امنیت فیزیکی و محیطی شود.

وقایع ضد امنیت فیزیکی در حوزه‌ی فناوری اطلاعات و ارتباطات دارای منشأهای مختلفی هستند. یکی از انواع تهدیدهای محیطی اقدامات مجرمانه است. اقدامات مجرمانه شامل سرقت یا دستکاری اطلاعات با مقاصد مالی یا ماجراجویانه است. علاوه بر این برخی مخاطرات امنیت فیزیکی با مقاصد سیاسی یا آرمانی صورت می‌پذیرد که در این صورت عنوان جنگ بر آن اطلاق می‌شود. اگرچه مخاطرات ایجاد شده برای سازمان‌ها در حوزه فیزیکی، چه در جرایم و چه در جنگ‌ها شامل مواردی چون دسترسی غیرمجاز یا تخریب زیرساخت‌ها، تجهیزات، خطوط ارتباطی و ابزارهای نظارت و کنترل است، اما مقصود عامل تهدید در انتخاب نحوه‌ی مقابله با آن اهمیت زیادی دارد. برخی سازمان‌ها روال‌های امنیتی را تنها برای مقابله با جرایم دارای انگیزه‌های مالی درنظر می‌گیرند. در نتیجه وقتی با مهاجمی مواجه شوند که اهداف سیاسی، آرمانگرایانه

یا ماجراجویانه دارد، توان مقابله با تهدید از آن‌ها سلب می‌شود. به عبارت دیگر برای تدوین یک برنامه‌ی جامع مقابله و بازیابی در حوزه‌ی امنیت فیزیکی، توجه به مقاصدی که مهاجم می‌تواند به عنوان یک دولت یا گروه متخاصم یا یک ماجراجو داشته باشد علاوه بر انگیزه‌های مالی ضروری است. از طرف دیگر گاهی ابزارها و سرمایه‌گذاری‌های دولت‌های متخاصم برای ایجاد آسیب در سازمان‌ها فراتر و به مراتب قوی‌تر از ابزارها و سرمایه‌گذاری‌های مجرمان و سارقان است و بنابراین راه‌های مقابله با این نوع از تهدیدها نیاز به صرف بودجه و توان بیشتری دارد.

برقراری امنیت فیزیکی شامل ملاحظاتی است که عبارتند از:

- جلوگیری از دستیابی غیر مجاز، وارد کردن صدمه و تداخل به اطلاعات سازمان در محیط‌های امن
- جلوگیری از تلف شدن و واردآمدن صدمه به دارایی ها و وقفه در کار تجهیزات سازمان
- جلوگیری از تساهل یا سرقت اطلاعات و فراوری اطلاعات
- استفاده از حفاظ های محیطی مناسب برای تأسیسات و تجهیزات فناوری اطلاعات و ارتباطات
- تجهیز ورودی‌های اماکن حیاتی، حساس و مهم به تجهیزات کنترل دسترسی
- برقراری سامانه رویداد نگاری و ممیزی در اماکن حیاتی، حساس و مهم
- رعایت اصل حداقل دسترسی شامل حیطه‌بندی و سطح‌بندی صلاحیت‌های دسترسی

- تأکید بر توجه به ضوابط امنیت فیزیکی به منظور استمرار فعالیت های کلیدی.
- تأکید بر کنترل محل های تحویل و ارائه اطلاعات تا در صورت امکان مجزا از دیگر درگاه‌ها باشند.
- تأکید بر مشخص بودن نحوه احراز اصالت برای استفاده از تجهیزات مورد استفاده
- تأکید بر تعبیه تجهیزات در محل مناسب و ایمن.
- تأکید بر حفظ تجهیزات از هر گونه صدمات ناشی از قطع یا خرابی منابع تغذیه. (ترجیحا استفاده از UPS).
- تأکید بر تعیین مناسب نوع سامانه های گرمایشی، سرمایشی و تهویه کننده(در نظر داشتن استانداردهایHVAC)
- تأکید بر مشخص کردن دقیق اماکن و تجهیزاتی که نیاز به تعیین امنیت وکنترل دارند.
- تأکید بر تعیین کردن سطح دسترسی به اماکن امن شناخته شده
- تأکید بر حفاظت از کابل کشی های برق، داده ها و تلفن.
- تأکید بر نگهداری تجهیزات، متناسب با دستورالعمل های سازنده یا مستندات ارائه شده.
- تأکید بر تدوین روند نگهداری و بایگانی رسانه ها و اسناد

- تأکید بر پیش بینی تسهیلاتی جهت کاهش آسیب های ناشی از سوانح طبیعی(مانند آتش سوزی، سیل، زلزله و....) در خط مشی مدیریت بحران
- تأکید بر تدوین روال های امن به منظور امنیت تجهیزات در هنگام استفاده از بیرون سازمان.
- تأکید بر پاک شدن اطلاعات از روی تجهیزاتی که مجدداً مورد استفاده یا در دسترس عموم قرار می‌گیرند.
- تأکید بر مشخص کردن نحوه و زمان پشتیبان‌گیری از داده‌های رسانه‌ها
- تأکید بر در نظر داشتن ملاحظات امنیتی در نگهداری و امحاء تجهیزات اسقاطی
- تأکید بر تدوین طرحی در مورد از رده خارج کردن تجهیزات
- تأکید بر خط مشی پاکسازی میز به منظور کاهش مخاطرات ناشی از دستیابی غیر مجاز و فقدان یا صدمه به اطلاعات.(یعنی تا حد امکان اطلاعات، مستندات و امکانات در معرض و دسترس قرار نگیرند)
- تأکید بر عدم جابجایی بدون هماهنگی تجهیزات، اطلاعات یا نرم افزار متعلق به سازمان
- تأکید بر پیروی از ملاحظات مدون حفاظتی در کلیه نقل و انتقال‌ها
- تأکید بر تدوین طرح به کارگیری و به حداقل رساندن انتقال رسانه های قابل انتقال (لپ‌تاپ‌ها، نوارها، کاست ها، CDها، فلاپی ها، گزارشات چاپ شده و...)

- تأکید بر مشخص کردن موقعیت تجهیزات و ابزار آلات داخل سازمانی مربوط به شبکه
- حفاظت تأسیسات فیزیکی در مقابل تصادف‌ها یا اختلالاتی که به دلیل حضور افراد مغرض پیش می‌آید.
- یک سامانه امنیت فیزیکی همیشه شامل تجهیزات کنترل دسترسی برای نظارت خودکار بر نقاط ورودی و یک سامانه هشدار بر مبنای حسگرهای مختلف است. سایر ملاحظات حفاظتی ممکن است منجر به استفاده از دوربین‌های مراقبتی و حفاظ‌های امنیتی نیز شود.

امنیت محیطی و فضای مجازی

برقراری امنیت، ایمنی و پایداری در هر مجموعه شامل مؤلفه‌های مختلفی است که با توجه به گسترش نفوذ فناوری اطلاعات و ارتباطات، یکی از این مؤلفه‌ها، فضای مجازی است. همراهی و یکپارچگی برنامه برقراری امنیت محیطی با برنامه‌ی امنیت فضای مجازی، اولین اولویت در تأمین امنیت محیطی و فیزیکی هر مجموعه به شمار می‌رود. باید توجه داشت که این همراهی و یکپارچگی آن‌چنان هم پیچیده نیست. چرا که می‌توان با استفاده از یک قاعده کلی این همراهی را تضمین نمود: هر دارایی مهم در فضای مجازی مبتنی بر تجهیزات و زیرساخت‌هایی است که امنیت فیزیکی و محیطی آن در برنامه امنیت محیطی باید تضمین شود. به عبارت دیگر بروز فاجعه در زیرساخت‌های فیزیکی فضای مجازی موجب مختل شدن فعالیت‌ها و خدشه‌دار شدن امنیت در فضای مجازی می‌شود. هم‌چنین بخش عمده‌ای از تهدیدات فضای مجازی ناشی از دسترسی فیزیکی به تجهیزات و سامانه‌های فناوری اطلاعات و ارتباطات است که معمولا از

دید مهندسان و متخصصان امنیت فضای مجازی، این بخش از تهدیدها یا نادیده گرفته می‌شود یا کمتر مورد توجه قرار می‌گیرد.

از طرف دیگر باید توجه کرد که در بسیاری از موارد مدیریت امنیت محیطی مبتنی بر ابزارها و نرم‌افزارهایی است که قواعد امنیت فضای مجازی در تهیه، نصب، راه‌اندازی، به کارگیری و پشتیبانی از آن‌ها باید مورد توجه قرار گیرد. به عنوان نمونه سامانه‌های کنترل دسترسی، نگهداری سوابق تردد و یا سامانه‌های تشخیص، اعلام یا اطفای حریق همگی مبتنی بر فناوری اطلاعات و ارتباطات بوده و امکان آسیب زدن به امنیت فیزیکی از طریق حملات فضای مجازی وجود دارد.

امنیت محیطی و برنامه بازیابی حوادث

دسته‌بندی سامانه‌ها و برنامه‌های حیاتی و اولویت‌بندی آن‌ها برای طرح‌ریزی برنامه بازیابی حوادث می‌تواند به عنوان یکی از منابع طبقه‌بندی دارایی‌ها در برنامه امنیت محیطی استفاده شود. در برنامه‌ی بازیابی حوادث لازم است دارایی‌ها و سرمایه‌هایی را که بیشترین میزان ریسک را در بروز حوادث دارند شناسایی و مطابق با الگوهای مدیریت بحران برای بازیابی آن‌ها پس از حوادث برنامه‌ریزی کرد. در واقع طبقه‌بندی و دسته‌بندی دارایی‌های سازمان در برنامه مدیریت بازیابی حوادث به عنوان گام اول تلقی می‌شود.

اگر بخواهیم مشابه بخش قبل یک قاعده کلی ارائه دهیم، می‌توانیم هر نرم‌افزار، شبکه یا فرآیندی را که بازیابی آن پس از بروز حوادث دارای اولویت است، یک هدف کلیدی در برنامه امنیت محیطی در نظر بگیریم. به عبارت دیگر رعایت ملاحظات امنیت فیزیکی و محیطی در خصوص دارایی‌های حیاتی در مراحل پیش، حین و پس از هر رویداد ناگوار موجب اجرای بهتر برنامه‌ی بازیابی حوادث در سازمان می‌شود.

اگرچه اقدامات مربوط به بازیابی حوادث در ابتدای بحران یا پس از آن آغاز می‌شود، اما فرآیند این اقدامات از پیش از بروز هر حادثه با برنامه‌ریزی در خصوص شناسایی و ارزیابی میزان ریسک دارایی‌ها و پیش‌بینی حوادث و در نظر گرفتن تمهیدات لازم برای زمان وقوع بحران و پس از آن شروع می‌شود. اقدامات حین بحران معمولا شامل فعالیت‌هایی است که آسیب‌ها را کاهش داده و مجموعه را برای بازیابی فعالیت‌ها و خدمات و به عبارت دیگر تداوم کسب و کار آماده می‌کند.

امنیت محیطی و برنامه تداوم کسب و کار

مطابق ادبیات پدافند غیرعامل برنامه تداوم کسب و کار را می‌توان برنامه‌ی حفظ پایداری زیرساخت‌ها دانست. بنابراین تدوین یک برنامه‌ی پدافند غیرعامل در هر سازمان مستلزم تهیه یک طرح تداوم کسب و کار در آن سازمان است. یکی از متداول‌ترین اجزای هر طرح تداوم کسب و کار، ایجاد یک سایت پشتیبان برای ارائه خدمات سازمان در صورت بروز مخاطره در سایت اصلی است. راه دیگر در اجرای این طرح، نگهداری اطلاعات پشتیبان نرم‌افزارها و دارایی‌های اطلاعاتی سازمان در مکان فیزیکی متفاوتی از سازمان اصلی است. همانطور که ملاحظه می‌کنید هر دوی این اقدامات به نوعی جزء ملاحظات امنیت محیطی تلقی می‌گردند.

البته باید توجه داشت که برنامه‌ی حفظ پایداری خدمات یا تداوم کسب و کار شامل موارد دیگری فراتر از ملاحظات محیطی، مانند راه‌اندازی خطوط دیگر ارائه خدمات یا تعریف فرآیندهای متفاوت برای ترمیم مسیرهای آسیب‌دیده در ارائه خدمات می‌شود.

ارزیابی نیازمندی‌های قانونی

باید در نظر داشت که برقراری یک برنامه تأمین امنیت محیطی علاوه بر تمام ملاحظات پیش‌گفته نیازمند ارزیابی و در نظر گرفتن نیازمندی‌های قانونی است. از آن‌جا که قلمرو فعالیت پدافند غیرعامل در خصوص زیرساخت‌های حیاتی، حساس و مهم کشور است، تأمین نیازمندی‌های قانونی در رسیدن به اهداف سازمان‌های موضوع این قلمرو نقش به سزایی دارد. با توجه به آن‌که تغییرات مختلف در همه‌ی ابعاد سامانه‌های فناوری اطلاعات و ارتباطات اعم از ظهور فناوری‌های جدید، ایجاد فرآیندهای نو و تعریف خدمات تازه با سرعت بسیار زیادی رخ می‌دهد، وجود قوانین و مقررات مختلفی که بتواند خود را با این تغییرات تطبیق دهد ضروری می‌نماید.

از طرفی عدم وجود قوانین و مقررات شفاف و دقیق منجر به سلب مسؤولیت تأمین‌کنندگان یا برپا کنندگان فضای سایبر از خود در قبال مخاطرات ایجاد شده می‌شود. بنابراین تعمیم قوانین مختلف در حوزه‌ی فضای حقیقی به مجازی با در نظر گرفتن ملاحظات مربوطه و نیز تدوین قوانین جدید مخصوص این فضاها به ضابطه‌مند کردن فرآیندها کمک نموده و از سردرگمی متولیان تأمین امنیت در مقابله با مخاطرات و شناسایی و برخورد با مجرمین جلوگیری می‌نماید.

یکی دیگر از ملاحظات قانونی در خصوص حوزه‌های فناوری اطلاعات و ارتباطات، حاکمیت نظام‌های قضایی متعدد بر یک زیرساخت یکپارچه است. به عنوان مثال اگر سازمانی دسترسی راه دور به سامانه‌های فناوری اطلاعات و ارتباطات خود را برای مدیران و کارکنان خود فعال نماید، امکان بروز مخاطراتی برای این سامانه‌ها از مکان‌هایی در خارج از قلمرو قانون کشور برای سامانه به وجود می‌آید. از آن‌جا محل وقوع جرم را نمی‌توان مطابق قوانین مرسوم در فضای حقیقی تعریف نمود، ممکن است تفاوت قانونی موجب عدم امکان پیگرد و برخورد با مجرم یا مجرمان شود.

به عنوان آخرین ملاحظه در این بخش به تفاوت مفهوم مالکیت و نظارت در حوزه‌های حقیقی و مجازی می‌پردازیم. اگرچه طبق قوانین مختلف موجود در اکثر کشورها، صاحبان یک کالا یا سامانه در قبال عملکرد خود در مورد آن کالا مختار هستند و تا زمانی که فعالیت مالک، مخل آزادی دیگران نشده، در خصوص عملکرد خود مورد پیگرد قرار نمی‌گیرند، اما یکپارچگی سامانه‌های فناوری اطلاعات و ارتباطات مفهوم مالکیت و اختیارات مالک را دچار تحولات ویژه نموده است. بررسی مفصل این تفاوت‌ها و نیازمندی‌های قانونی در این خلاصه نمی‌گنجد و بیان این ملاحظات تنها برای آشنا کردن مخاطبان با آن‌ها صورت گرفته است.

سازماندهی

مدیریت هر فعالیت اجرایی نیازمند سازماندهی و ایجاد ساختار مناسب است. از آن‌جا که برقراری امنیت محیطی نیاز به فعالیت‌های اجرایی دارد، برای موفقیت در برقراری امنیت محیطی در هر سازمان باید ساختار لازم طراحی و پیاده‌سازی شود.

هیچ الگوی ثابتی را نمی‌توان به عنوان ساختار اجرایی مناسب همیشه برای همه‌ی سازمان‌ها پیشنهاد کرد. برای استقرار نظام امنیت در سازمان باید با توجه به نوع مأموریت، فرآیندهای سازمانی، فناوری، شرایط و موقعیت‌های داخلی و خارجی ساختار مناسب را استفاده کرد. عواملی مانند ابعاد، قدمت و پیچیدگی سازمان نیز در طراحی ساختار مناسب باید در نظر گرفته شوند تا نیل به اهداف سازمان با این ساختار تسهیل شود.

با توجه به آن‌چه گفته شد، حوزه‌ی فناوری اطلاعات و ارتباطات و همچنین حفاظت از زیرساخت‌های آن با توجه به ماهیت خود نیازمند ساختاری خاص، منطبق با ویژگی‌های این حوزه است.

ساختار نوین

فناوری اطلاعات اولین بار در اواسط قرن بیستم توسط شرکت‌های بزرگی مثل «آی.بی.ام» مطرح شد و تولید نرم‌افزارهایی که کارایی سازمان را بالا ببرد در دستور کار قرار داشت. به همین دلیل نرم‌افزارهایی مانند سامانه انبارداری و سامانه پرداخت حقوق و دستمزد و یا سامانه حسابداری عرضه شد. با استفاده از این نرم‌افزارها هزینه سازمان‌ها کاهش یافته و در نتیجه کارایی آن افزایش می‌یافت.

در مرحله دوم حیات فناوری اطلاعات موضوع اثربخشی مورد توجه قرار گرفته و استفاده از این فناوری برای افزایش احتمال دسترسی به اهداف مطرح می‌شود و سامانه‌های اطلاعاتی جدیدی مثل سامانه‌های پشتیبان تصمیم (DSS) و سامانه‌های خبره (ES) برای کمک به مدیران و تحلیلگران ارائه می‌شود. به عنوان مثال، یک پزشک با استفاده از یک سامانه خبره مطمئن می‌شود که در جریان مداوای بیمار، مورد مهمی از قلم نمی‌افتد.

در سال‌های آخر قرن بیستم، فناوری اطلاعات وارد مرحله سوم عمر خود شده و با ورود سامانه‌های اطلاعاتی راهبردی، تحولی عظیم به وقوع پیوست. در این مقطع، وضعیت به گونه‌ای شده که سازمان‌ها بدون استفاده از این نوع سامانه‌ها قادر به رقابت نیستند و در نتیجه ی بی‌توجهی به آن، بعض ا دچار اضمحلال می‌شوند. بنابراین، می‌توان گفت امروزه ساختار سازمان‌ها بر اساس شبکه‌ها و سامانه‌های اطلاعاتی و ارتباطی آن‌ها شکل می‌گیرد.

هدف تئوری سازمان، تسهیل در ارتباطات، هماهنگی و کنترل است. در گذشته برای تحقق این سه هدف، سازمان‌ها مجبور به افزایش تفکیک افقی و عمودی، ایجاد واحدهای سازمانی جدید و پراکنده کردن فعالیت‌های سازمانی از نظر جغرافیایی بودند. با ظهور و بکارگیری فناوری اطلاعات، مدیران با استفاده از سامانه‌های اطلاعاتی می‌توانند به طور اثربخش فعالیت‌ها را هماهنگ و کنترل نمایند و نیاز به مدیران میانی را کاهش دهند. در نتیجه ساختار سازمانی مسطح‌تر

خواهد شد. همچنین، با استفاده از فناوری اطلاعات، محدودیت‌های فیزیکی و مکانی دیگر نقشی در تعیین ترتیبات ساختاری نخواهند داشت.

باید توجه داشت که سرعت بالای تغییر در محیط سازمان‌ها و نیز رشد و توسعه و عرضه‌ی سامانه‌های جدید فناوری اطلاعات و ارتباطات، پویایی و انعطاف‌پذیری بیشتری را در ساختار سازمان‌ها می‌طلبد. از طرف دیگر انعطاف‌پذیری ساختار سازمانی، قابلیت نوآوری و برخورد فعال در مقابله با تغییرات محیطی را به عنوان یک مزیت راهبردی برای سازمان به ارمغان می‌آورد.

چالش‌های ورود فناوری اطلاعات و ارتباطات به ساختار سازمان و امنیت

پیش از تحولات نیمه‌ی دوم قرن بیستم، اکثر سازمان‌ها ساختاری هرمی داشتند. به عبارت دیگر ساختار سازمانی بر اساس سلسله مراتبی بود که در آن مدیر سازمان، به تنهایی تصمیم‌گیرنده‌ی سازمان بود و جریان دستورات و سامانه نظارت و کنترل از بالا به پایین در سازمان جریان داشت. در نقطه‌ی مقابل، جریان اطلاعات و گزارش‌های مختلف از پایین به بالا و از کلیه‌ی سطوح به مدیر ارشد سازمان منتقل می‌شد. این ساختار باعث می‌شد که هم مرزهای سازمان و محیط از یک سو و هم حیطه‌بندی و وظایف هر بخش در سازمان نیز از سوی دیگر کاملا مشخص باشند. در نتیجه برقراری امنیت چه در برابر تهدیدات محیطی و چه در داخل سازمان با ارائه‌ی دستورالعمل‌های امنیتی از بالا به پایین امکان‌پذیر بود. از طرف دیگر حیطه‌بندی در سطوح مختلف سازمان، و دسترسی محدود کارکنان سطوح پایین‌تر به اطلاعات و سایر منابع سازمان، خود باعث ایجاد امنیت بیشتری برای سازمان می‌گردید.

با گسترش استفاده از فناوری‌های نوین به خصوص فناوری اطلاعات و ارتباطات و تحولات اساسی ایجاد شده در ساختار سازمان‌ها، شکل ارتباطی در ساختارهای جدید ماهیتاً با نوع ارتباط بالا به پایین در ساختارهای هرمی متفاوت

شده است. در ساختارهای شبکه‌ای جدید سازمان‌ها که در بخش قبل به آن اشاره شد، جریان اطلاعات دیگر نه به صورت از بالا به پایین که به صورت دو طرفه در یک شبکه برقرار می‌شود. از طرف دیگر تعیین مرز منطقی سازمان به سادگی ساختارهای هرمی قابل تعریف نیست. در نتیجه برقراری امنیت و نظارت بر آن با اجرای دستورالعمل‌های از پیش تعیین شده امکان‌پذیر نیست. در این ساختار جدید باید حفظ امنیت و رعایت ملاحظات امنیتی به صورت ارزش‌های سازمانی و استراتژی سازمان تعریف شود. بدیهی است که سامانه‌های نظارتی بر برقراری امنیت باید به صورت یک واحد با مدیریت متمرکز و پراکنده در کل ساختار شبکه‌ای وجود داشته باشد.

یکی دیگر از نتایج گسترش استفاده از فناوری اطلاعات و ارتباطات ایجاد سازمان‌هایی است که به صورت جغرافیایی متمرکز نیستند. سازمان‌هایی که دفاتر متعددی در نقاط مختلف یک کشور یا در کشورهای مختلف دنیا دارند، نمونه‌ای از این دسته سازمان‌ها هستند. از طرف دیگر بسیاری از سازمان‌های مبتنی بر فناوری اطلاعات و ارتباطات قسمت عمده‌ای از کارهای خود را توسط کارکنان در خانه انجام می‌دهند. این گستردگی جغرافیایی و هم‌چنین پراکندگی کارکنان یکی دیگر از چالش‌های برقراری امنیت در سازمان است.

هم‌چنین با توجه به سرعت بالای تغییر و رشد فناوری اطلاعات و ارتباطات و به دنبال آن ساختارها و فرآیندهای سازمانی، تهیه دستورالعمل‌های امنیتی ثابت برای سازمان تقریبا غیرممکن شده است. از طرف دیگر نظارت بر امنیت سازمانی پویا در همه‌ی ابعاد نیازمند پویایی و دانش‌محوری مسؤولان امنیتی سازمان است.

برون‌سپاری

یکی دیگر از مفاهیمی که از نیمه‌ی دوم قرن بیستم در حوزه مدیریت سازمان‌ها مطرح شد، بحث برون‌سپاری خدماتی است که به عنوان هسته‌ی اصلی کسب و کار سازمان به حساب نمی‌آیند. این مفهوم که با ایجاد سازمان‌های خدمت محور رواج بیشتری یافته، در اکثر سازمان‌های بزرگ به کارگرفته شده است. در خصوص امنیت و به خصوص امنیت محیطی نیز مانند بسیاری دیگر از سرویس‌های مورد نیاز سازمان‌ها باید بررسی شود که آیا امکان برون‌سپاری وجود دارد یا خیر.

با توجه به حوزه بحث که برون‌سپاری خدمات امنیت در سازمان‌های مبتنی بر فناوری اطلاعات و ارتباطات است، برخی از ملاحظاتی که در بررسی برون‌سپاری خدمات موردنیاز سازمان باید مدنظر قرار گیرد، در ادامه بحث می‌شود.

آن‌چه در تعیین امکان برون‌سپاری یک سرویس در ابتدا باید مورد بررسی قرار گیرد، بحث هزینه، فایده برون‌سپاری یک فعالیت است. بدیهی است برون‌سپاری خدماتی که هزینه داخلی بودن آن‌ها بیشتر از فایده‌ای است که می‌رسانند، برای سازمان‌ها اغلب مناسب است.

یکی دیگر از عواملی که باعث برون‌سپاری خدمات مورد نیاز سازمان می‌شود، تخصص بالای مورد نیاز برای ارائه این خدمات است. چرا که از طرفی امکان پرداخت هزینه‌های بالای استخدام دائم نیروی متخصص آن خدمت وجود ندارد و از طرف دیگر تخصص بالای افراد در ارائه این نوع خدمت‌ها، ناشی از ارائه سرویس به سازمان‌های مختلف است.

عامل بعدی مؤثر در برون‌سپاری خدمات سازمان، اندازه سازمان است. به عبارت دیگر قدمت، ساختار، تعداد پرسنل و حجم فعالیت سازمان‌ها در تصمیم‌گیری برای برون‌سپاری خدمات مؤثر است.

آخرین عاملی که در این مختصر به آن می‌پردازیم، بحث اهمیت سرویس و تأثیر آن در تداوم کسب و کار اصلی سازمان است. هیچ سازمانی حاضر نیست، سرویسی را که نقش مهمی در تداوم کسب و کار خود دارد برون‌سپاری کند. از طرف دیگر برخی تعهدات سازمان‌ها چه در بخش‌های خصوصی و چه در بخش دولتی به نهادهای سیاست‌گزار و نظارتی در اهمیت برخی سرویس‌ها مؤثر است.

یکی از محدودیت‌های برون‌سپاری که در موفقیت یا عدم موفقیت این دسته از فعالیت‌ها مؤثر است، میزان آشنایی با فرهنگ سازمانی و دسترسی به منابع اطلاعات سازمان است. عموما تمام سازمان‌ها در مقابل ایجاد دسترسی به اطلاعات سازمانی برای شرکت‌ها و مشاوران سازمان مقاومت می‌کنند و از طرف دیگر عدم آشنایی سازمان‌های ارائه دهنده خدمات با شرایط و فرهنگ سازمان موجب بروز مشکلات پیش‌بینی نشده‌ای در تعامل سازمان‌ها و موفقیت در برون‌سپاری خدمات می‌شود.

یکی از عوامل مؤثر در تصمیم‌گیری برای برون‌سپاری خدمات مورد نیاز سازمان، به خصوص در سازمان‌های فناوری محور، داشتن تخصص بالا و مجریان حرفه‌ای در برخی از این خدمات است. تغییرات سریع فناوری اطلاعات و ارتباطات موجب می‌شود تا مدیران اقدام به برون‌سپاری خدمات این حوزه از جمله امنیت کنند.

همان‌طور که قبل از این در خصوص تأمین امنیت مراکز حیاتی و حساس اشاره شد، نقش بودجه و تأمین مالی در اجزای پروژه‌های امنیتی، با توجه به شرایط ویژه‌ی این مراکز کم‌رنگ‌تر است. در خصوص برون‌سپاری خدمات امنیت فناوری اطلاعات نیز به دلیل حساسیت این مراکز و علی‌رغم تخصصی بودن حوزه‌های مختلف امنیت، لازم است در برون‌سپاری این دسته از فعالیت‌ها ملاحظات خاصی در خصوص اهمیت اطلاعات و فرآیندهای سازمان لحاظ شود

و در صورت لزوم این فعالیت‌ها به سازمان تخصصی دیگری وابسته به سازمان اصلی واگذار شود.

یک طرح امنیت محیطی در مراکز فناوری اطلاعات و ارتباطات شامل مراحل مختلفی است. فارغ از بررسی دقیق چرخه‌ی تأمین امنیت، اولین مرحله از هر پروژه، طراحی مفهومی سامانه امنیتی است. در ادامه این مرحله، پروژه وارد فاز طراحی سناریوها و تأمین تجهیزات می‌شود. نصب و راه‌اندازی سامانه و نگهداری آن به عنوان مراحل بعدی خواهد بود. اگرچه بهتر است که در کلیه این مراحل در مراکز حیاتی، حساس و مهم، برون‌سپاری صورت نگیرد، اما در صورتی که امکان چنین عملی فراهم نبود، لازم است مراحل تصب و راه‌اندازی و نگهداری به صورت درونی انجام شود و در ضمن در کلیه‌ی مراحل طرح، انتقال دانش نیز صورت پذیرد.

جایگاه مدیر امنیت

با توجه به آن‌چه در خصوص اهمیت و نقش امنیت در سازمان اشاره شد، می‌توان نتیجه گرفت که برقراری امنیت جزء وظایف مدیریت سازمان است. به عبارت دیگر تعهد مدیریت سازمان به برنامه‌های پدافند غیرعامل در کلیه‌ی حوزه‌ها از جمله فناوری اطلاعات و ارتباطات، تنها از طریق اجرای این برنامه‌ها توسط مدیر ارشد سازمان تأمین می‌شود. به همین دلیل لازم است کلیه برنامه‌ها و فرآیندهای پیشنهادی در این حوزه مورد بررسی و تأیید مدیریت سازمان قرار گیرد و سپس توسط وی برای اجرا به کلیه بخش‌های سازمان ابلاغ شود.

با توجه به این ملاحظه می‌توان مدیر امنیت را نماینده مدیریت سازمان در خصوص مسایل امنیتی و پدافندی دانست. در این صورت لازم است کلیه برنامه‌های امنیتی پس از تأیید و ابلاغ مدیریت سازمان توسط مدیر امنیت در کلیه

بخش‌ها اجرا شده و کلیه مدیران و بخش‌های سازمان در اجرای دستورالعمل‌ها و فرآیندها با مدیر امنیت همکاری کنند.

معماری امنیت

در آخرین بخش از این نوشته لازم است به یکی از مفاهیم جوان در حوزه سازمان و امنیت آن بپردازیم. این مفهوم، معماری امنیت در سازمان نام دارد.

منظور از معماری تعیین ساختار کلی و نمای روش‌هایی است که سازمان و سامانه را در هر حوزه به اهداف نهایی خود می‌رساند. بنابراین حوزه‌ی معماری علاوه بر وجوه ساختاری، دربردارنده‌ی وجوه رفتاری و فرآیندی نیز هست.

معماری یک سامانه از جنس تخیل است. به این مفهوم که این معماری باید پیش از برداشتن هر قدمی برای راه‌اندازی سامانه صورت گیرد. از طرفی این مفهوم هم بسته به نوع نگاه معمار سامانه و هم بسته به نوع تصور اوست. مهمترین کارکرد معماری ایجاد محملی برای ادراک در هنگام طراحی، مدیریت و نگهداری سامانه و همچنین نظامی برای انتقال این ادراک است. اگر معماری سامانه مورد توافق و تأیید کلیه تصمیم‌گیران سامانه قرار گیرد، بستری شکل می‌گیرد که به کارآیی مطلوب‌تر، ساختاری به روزتر، کیفیت و سازگاری بیشتر وانعطاف‌پذیری بالاتر در مقابل تغییرات محیطی کمک می‌نماید.

مؤلفه‌های اساسی معماری عبارتند از :

- تجرید: معماری باید از مسایل جزئی که در ساختار کلی اثر جدی ندارد، منفک شود.
- نگاه عقلانی[1]: معماری باید عقلانیت محوری موجود در یک سامانه، و فلسفه وجودی عناصر و مکانیزم‌ها را تبیین کرده و نشان دهد.

[1] Rational

- ساختمان مفهومی: معماری باید مفاهیم بنیان کننده سامانه و ساختار آنها را تبیین کند.
- یکپارچگی نگاه: تبیین یک‌پارچه کل سامانه یا موضوع خاص در کل سامانه، و ارتقاء نقطه دید.
- کل گرائی: تبیین یک نگاه کل گرا و بسیط (نه مرکب) از سامانه و تبیین روح و مغز سامانه.
- هم بندی مولفه ها: تبیین عناصر محوری و هم بندی و محورهای ساختار و رفتار.

می‌توان معماری سامانه و سازمان را پیاده‌سازی عملی نگرش سامانهی و دیدگاه‌های کل‌نگر در حوزه عملیاتی دانست.

مفهوم معماری در حوزه امنیت سامانه، با مفهوم معماری ساختمان قابل مقایسه است . نقشه‌های ساختمان شامل برداشت‌های اولیه‌ای در مورد برق ، لوله‌کشی، کابل‌کشی، ورودی‌ها، خروجی‌ها، پله‌ها و آسانسورها و ... است. به علاوه، نقشه‌ها دیدگاه‌هایی را در مورد طراحی کلی ساختمان شامل ساخت از جمله تعداد طبقات، دیوارهای درونی و بیرونی و کیفیت پشت بام ارایه می کند. همچنین نقشه‌های دیگری که در سطح پایین‌تر نشان دهنده چیدمان تجهیزات به کار رفته و ساخت مواد موردنیاز است، این معماری را تکمیل می‌کند.

معماری امنیت نیز از اصول مشابه در معماری ساختمان استفاده می‌کند تا بنیان درستی را برای تصمیم‌گیری درباره وضع و اجرای قوانین، خرید و نصب تجهیزات و رعایت ملاحظات ایجاد کند.

زیرمعماری‌های تولیدشده در هنگام ایجاد طرح معماری اطلاعات دقیقا شبیه به همان نقشه‌های معماری ساختمان هستند. آنها نشان دهنده راه‌هایی هستند که

امنیت، ایمنی و پایداری زیرساخت‌ها و خدمات و فعالیت‌های حال و آینده سازمان را ضمانت می‌کنند.

بر اساس استاندارد IEEE 1471 معماری سامانه تجسمی از اجزاء و روابط بین آن‌ها و طراحی و تکامل آن‌ها است. بر این اساس معماری یک سازمان شامل زیر بخشی به نام معماری امنیت خواهد بود که بر خلاف بسیاری از زیربخش‌های دیگر سامانه حوزه اثرش محدود نیست. معماری امنیت، روح فعالیت و ضامن بقا و پایداری سامانه است و در کلیه فعالیت‌های مختلف سامانه نفوذ و نمود دارد.

معماری امنیت یک سامانه یا سازمان شامل سه بخش اساسی است که این بخش‌ها عبارتند از:

- مبانی فلسفی، شالوده‌ها و اصول کلی امنیت سازمان
- فرآیندها و سازوکارهای برقراری امنیت، ایمنی و پایداری سازمان و فعالیت‌های آن
- ساختار کلان عناصر تشکیل دهنده و روابط و سازکارهای ارتباطی این عناصر