زمان دریافت مقاله: ۹۵/۵/۱۸
زمان پذیرش مقاله: ۹۵/۷/۲۲

بررسی جایگاه امنیت رایانه‌ای در کسب و کار دیجیتال

سعید کاظم پوریان
کارشناس ارشد مهندسی فناوری اطلاعات، دانشکده فنی و مهندسی، دانشگاه شاهد، تهران، ایران
پست الکترونیکی: saeed.kazem.313@gmail.com

چکیده

با ظهور هر موضوع و فناوری جدید در دنیای مجازی، مبحث امنیت یکی از مهمترین مسائل مربوطه به آن خواهد بود. کسب و کار دیجیتال به دنبال کسب و کار الکترونیکی، یکی از مباحث نوظهور در دنیای فناوری اطلاعات است و امنیت رایانه‌ای، بنیان کسب و کار و نوآوری دیجیتال می‌باشد. در این محیط، سازمان‌های فناوری اطلاعات، زیرساخت محدودی را تحت نظر خود دارند و بزرگ‌ترین چالش‌های امنیتی آن‌ها مربوط به خدمات و اطلاعات خارج از کنترل آن‌ها خواهد بود که باعث به وجود آمدن مخاطرات امنیتی جدیدی برای سازمان‌ها می‌شود. هدف از این پژوهش، شناخت حوزه‌هایی است که برای مدیریت چنین مخاطراتی و در نتیجه موفقیت در مدیریت امنیت در دنیای دیجیتال باید مورد توجه قرار گیرند. در همین راستا در سال‌های اخیر تحقیقاتی انجام گرفته است تا به تبیین عوامل موفقیت امنیت رایانه‌ای در دنیای کسب و کار دیجیتال بپردازند. در این پژوهش، تحقیقات مؤسسه گارتنر در این حوزه بررسی شدند و مشخص شد که خصوصیات کسب و کار دیجیتال باعث تغییر برخی مدل‌ها و روش‌های مدیریت در زمینه امنیت شده است. در نهایت نتایج پژوهش نشان داد که رهبری و حاکمیت، محیط تهدید جدید، امنیت رایانه‌ای در کسب و کار و دنیای جدید و تغییر فرهنگی، ۵ عاملی هستند که برای موفقیت در زمینه امنیت رایانه‌ای کسب و کار دیجیتال باید به آن‌ها توجه کرد.

واژه‌های کلیدی: کسب و کار دیجیتال[1]، امنیت رایانه‌ای[2]، امنیت دیجیتال[3].

1- Digital Business
2- Cybersecurity
3- Digital Security

۱. مقدمه

کسب و کار دیجیتال، زیســت‌بوم خارجی گسترده‌تر و چالش‌های جدیدی در دنیــای دیجیتال به همراه دارد و امنیت رایانــه‌ای، یک بخش حیاتی آن اســت. دامنه امنیت رایانه‌ای در حال گســترش است و در حال تبدیل به امنیت دیجیتال می‌باشــد (شــکل ۱). به دلیل گذار سازمان‌ها به ســمت کسب و کار دیجیتال، رفع این کمبود که زیرساخت و خدمات خارج از کنترل ســازمان‌ها، مســتقیماً زیر نظر آن‌ها باشــد، مســتلزم آن اســت که امنیت رایانه‌ای به آن بپــردازد. ایمنی، نقطه مشــترکی میان فنــاوری و دنیای فیزیکی اســت (فناوری اطلاعات، فناوری عملیاتی، اینترنت اشیاء). مخاطرات دیجیتال، سازمان‌ها را به چالش می‌کشند و انتظار خســارات بیش‌تری نیز می‌رود [۱]. در پژوهشی در ســال ۲۰۱۶ از مدیران غیر فناوری اطلاعات، ۷۱٪ آن‌ها گفته‌اند که نگرانی‌ها در مورد امنیت رایانه‌ای، مانع نوآوری در سازمان‌های آن‌ها می‌شود [۲].

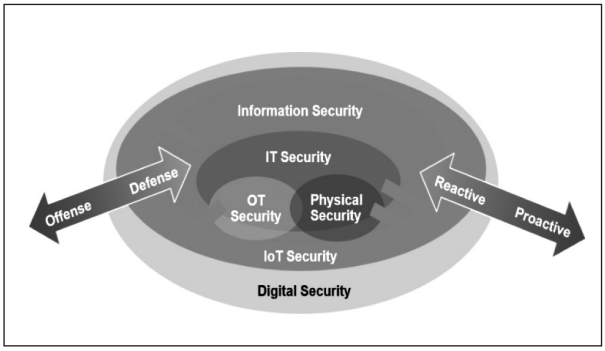
اطلاعــات و وقایع در فرهنگ، رفتار و فناوری، ملزم به تغییر اســت. مدیران امنیت، بیش‌تر شبیه مدیران اطلاعاتی و مشــاوران مورد اعتماد کار خواهند کرد، زیرا بر اساس پژوهشــی در مؤسسه گارتنر[4]، فناوری اطلاعات در بخش کسب و کار تبدیل به بخش اصلی خواهد گشت [۱]:

– در ســال ۲۰۱۸، ۲۵٪ از ترافیک داده‌های شــرکت‌ها مستقیماً از دســتگاه‌های سیار ابر می‌رود و از کنترل‌های امنیتی شرکت‌ها عبور می‌کند.

– در ســال ۲۰۲۰، ۶۰٪ کســب و کارهــای دیجیتال به دلیل ناتوانی تیم‌های امنیت فنــاوری اطلاعات در مدیریت مخاطرات دیجیتال، متحمل شکست خدمات عمده می‌شوند.

– در سال ۲۰۲۰، ۶۰٪ بودجه امنیت اطلاعات شرکت‌ها به رویکردهای تشــخیص و پاسخ ســریع تخصیص داده می‌شــود، در حالی که در سال ۲۰۱۶، این رقم چیزی کم‌تر از ۳۰٪ است.

سازمان‌ها خواهند آموخت که با سطوح قابل پذیرشی

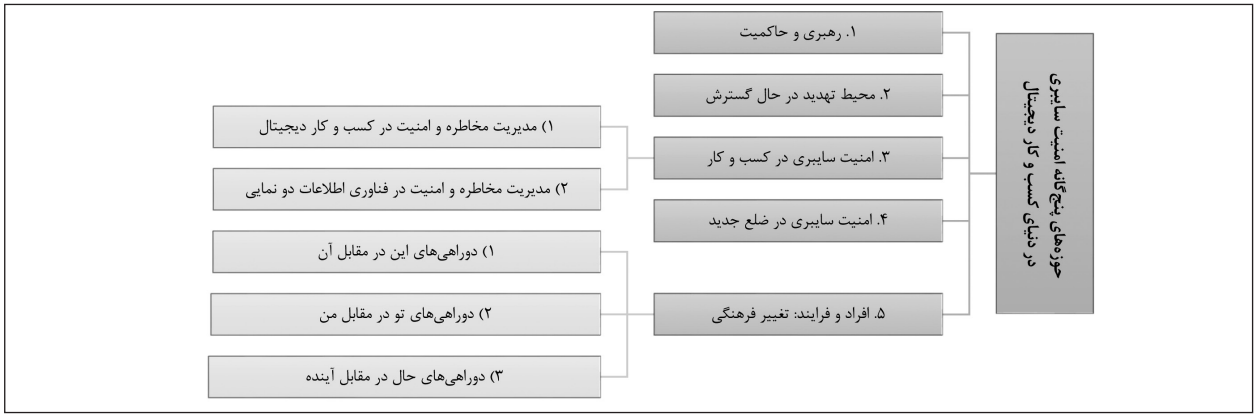


شکل۱: تبدیل دامنه امنیت رایانه‌ای به امنیت دیجیتال [۱]

از مخاطــرات دیجیتال به حیات ادامه دهند، زیرا واحدهای کسب و کار در کشف نیازهای امنیتی و توان اجرایی خود، نوآوری خواهند داشت. اخلاق دیجیتال، تجزیه و تحلیل و تمرکز، به اندازه کنترل‌هــای فنی مهم خواهند بود. گارتنر ۵ حوزه کلیدی را برای امنیت رایانه‌ای موفق در کســب و کار دیجیتال معرفی کرده است [۳]: ۱– رهبری و حاکمیت، ۲– محیط تهدید در حال گســترش، ۳– امنیت رایانه‌ای در کســب و کار، ۴– امنیت رایانه‌ای در ضلع جدید و ۵– افراد و فرآیند: تغییر فرهنگی. در این پژوهش ســعی شده است مروری بر این ۵ مورد انجام گیرد تا مشــخص شود برای داشــتن یک راهکار امنیت رایانه‌ای موفق در دنیای کسب و کار دیجیتــال، چه نکاتی باید رعایت شــود تا مخاطرات مربوط به دنیای دیجیتال به حداقل برسد. همچنین با توجه به تهدیــدات جدیدی که در این حوزه وجود دارد، تغییرات و آموزش‌های جدید نیز لازم می‌باشــد که در این پژوهش به شــرح این موارد نیز می‌پردازیم. همچنین در هر یک از حوزه‌ها نســبت به محیط‌های کسب و کار قبلی، تغییراتی حاصل شــده است و در برخی موارد مدل‌های جدیدی نیز ارائه گردیده است که بیشتر این موارد مربوط به تهدیدات جدید موجود در کســب و کار دیجیتال می‌باشــد. در این پژوهش این تغییرات و مدل‌ها نیز بررســی می‌شــوند تا مشــخص گردد که برای مدیریت این تغییرات، نیاز به چه کنترل‌ها، فرآیندها، روش‌ها و استانداردهایی داریم.

۲. امنیت رایانه‌ای موفق در کسب و کار دیجیتال

4- Gartner



شکل۲: حوزه‌های پنج‌گانه امنیت رایانه‌ای در دنیای کسب و کار دیجیتال

در این بخش به شرح هر یک از حوزه‌های پنج‌گانه امنیت رایانه‌ای در دنیای کسب و کار دیجیتال پرداخته می‌شود تا مشخص گردد برای موفقیت در این موضوع، لازم است به چه مسائلی توجه شود و نسبت به محیط‌های قبلی کسب و کار، چه تغییراتی باید حاصل گردد تا سازمان‌ها در آینده قادر به حل مشکلات امنیت رایانه‌ای خود باشند و کارآیی و اثربخشی خود را در دنیای کسب و کار دیجیتال از دست ندهند (شکل ۲).

۲-۱ رهبری و حاکمیت

وقتی به موضوع مخاطرات امنیت رایانه‌ای و فناوری در کسب و کار دیجیتال پرداخته می‌شود، مسلماً بحث بهبود رهبری و حاکمیت مهم‌تر از توسعه ابزار و مهارت‌های فناوری است. تصمیم‌گیری، اولویت‌بندی، تخصیص بودجه، سنجش، گزارش‌دهی، شفافیت و پاسخ‌گویی، مشخصات مهم برنامه موفق هستند که نیاز به نگهداری را با نیاز به حفاظت و نیاز به اداره کسب و کار متناسب می‌سازند. در حال حاضر نسبت به ۲۰ سال پیش، همه‌چیز برای مدیران امنیتی و واحدهای امنیتی متفاوت است. آن‌ها دارای سطح جدیدی از منابع هستند، اما به همراه آن، انتظارات جدیدی نیز برای اجرا وجود دارد. سازمان‌ها از مدل‌های جدیدی مانند ابر، ابزارهای سیار و اینترنت اشیاء استفاده می‌کنند که باید از آن‌ها حفاظت کنند، اما این امر مستلزم فناوری‌های جدید است. سازمان‌ها روش‌های جدیدی مانند فناوری اطلاعات دونمایی[5] نیز برای فعالیت دارند، اما این امر نیز مستلزم مهارت‌ها و رویکردهای جدید است. در نهایت ذکر این نکته مهم است که واحدهای امنیت، کنترل کم‌تری روی بسیاری از فعالیت‌ها دارند، زیرا راه‌های ایجاد و استفاده از خدمات فناوری اطلاعات گسترده‌تر می‌شوند [۱].

۲-۲ محیط تهدید در حال گسترش

تهدیدهای پیشرفته به گسترش ادامه می‌دهند. تغییرات در دستگاه‌ها و خدمات رایانشی که توسط کسب و کار دیجیتال به وجود آمده، به شکل‌دهی چشم‌اندازهای مخاطره و امنیت ادامه می‌دهد. شفافیت کسب و کار و تولید ارزش دیجیتال، رهبران امنیت و مخاطره را به سمت توسعه تجارب امنیتی برای تحمل‌پذیری کسب و کار هدایت می‌کند [۴].

تغییرات مهم در اصول فناوری اطلاعات و کسب و کار که توسط رایانش ابری، رایانش سیار، رسانه‌های اجتماعی و پایگاه‌های داده بزرگ انجام گرفته است، باعث به وجود آمدن بازاریابی دیجیتال جدید، وابستگی روزافزون کسب و کارها به تجزیه و تحلیل‌های سطح بالا، اتصال بی‌سیم همگانی و رایانش ابری شده است که پاسخ‌گویی سریع به درخواست‌های کسب و کار دیجیتال را نتیجه می‌دهد [۴].

مفهوم دیجیتال و رقابت برای آن در حال تغییر مدیریت امنیت و مخاطرات سازمانی است. مدل سنتی که

5- Bimodal IT

طی چند دهـــه برای امنیت فناوری اطلاعات در نظر گرفته می‌شد شامل محرمانگی، جامعیت و دسترس‌پذیری بود. در اکثر ســـازمان‌ها، چرخه مداوم شکســـت‌ها در امنیت رایانه‌ای باعث افزایش ســـطح مخاطره شـــده است و اکثر آن‌ها تا ســـال ۲۰۱۵ نتوانســـتند این مخاطرات را به شکل اساســـی بهبود دهند. این مدل هنوز هم کاربردی است اما دیگر کافی نیست [۵].

استفاده روزافزون از فناوری دیجیتال در ساختمان‌ها، شـــبکه‌های برقـــی، ســـامانه‌های حمـــل و نقـــل و ســـایر زیرســـاخت‌های حیاتی، این امر را ضروری ساخته است که ضلع دیگری به نام ایمنی نیز به مدل قبلی اضافه گردد. این اتفاق توسط اینترنت اشیاء نیز سرعت پیدا کرده است. محرمانگی، جامعیت، دسترس‌پذیری و ایمنی، اصول جامع امنیت رایانه‌ای برای ســـازمان‌ها در ســـال ۲۰۲۰ خواهند بود و ضلـــع جدیدی به نام ایمنی به مثلـــث امنیت، اضافه خواهد شـــد [۴].در حال حاضر رهبـــران مخاطره و امنیت رایانه‌ای باید مسئولیت فراهم کردن ایمنی را برای افراد و محیط آن‌ها بپذیرند و یا حداقل با سایر عملیات امنیتی در فراهم‌سازی ایمنی شرکت نمایند [۶].

۲-۳ امنیت رایانه‌ای در کسب و کار

کسب و کار دیجیتال با سرعت بیش‌تری نسبت به کسب و کار ســـنتی حرکت می‌کنـــد و رویکردهای ســـنتی امنیت که بـــرای حداکثر کنتـــرل طراحی شـــده‌اند، دیگر در عصر جدید نوآوری دیجیتال، جواب‌گو نیســـتند. فرصت، توسعه، تصمیم‌گیری و انتظارات کسب و کار باید با یک روش بموقع و کارآمد اداره شـــوند که مستلزم مهارت‌ها و تجارب جدید است. برنامه‌ها تکامل می‌یابند و فناوری اطلاعات دونمایی و ظهور پروژه‌های نوع-۲ [۶] در مدیریت مسیر اصلی، مستلزم رویکردی جدید در امنیت رایانه‌ای می‌باشد [۱].

۲-۳-۱.مدیریت مخاطره و امنیت در کسب و کار دیجیتال

کســـب و کار دیجیتـــال، اصـــول اساســـی مدیریت مخاطرات و امنیت اطلاعات را به چالش می‌کشد. رهبران مخاطره و امنیت باید مخاطرات مربوط به نوآوری کسب و کار را درک کننـــد و حفاظـــت از شـــرکت را با نیاز به پذیرش رویکردهای نوآورانه فناوری متعادل سازند [۶]. پذیرش روزافزون رویکردهای کسب و کار دیجیتال، در حال تغییر دادن چشـــم‌انداز حاکمیتی و کنترلی فناوری اطلاعات ســـنتی اســـت. دو مشـــخصه مهم کسب و کار دیجیتال، کنترل‌های مرسوم فناوری اطلاعات را به چالش می‌کشند:

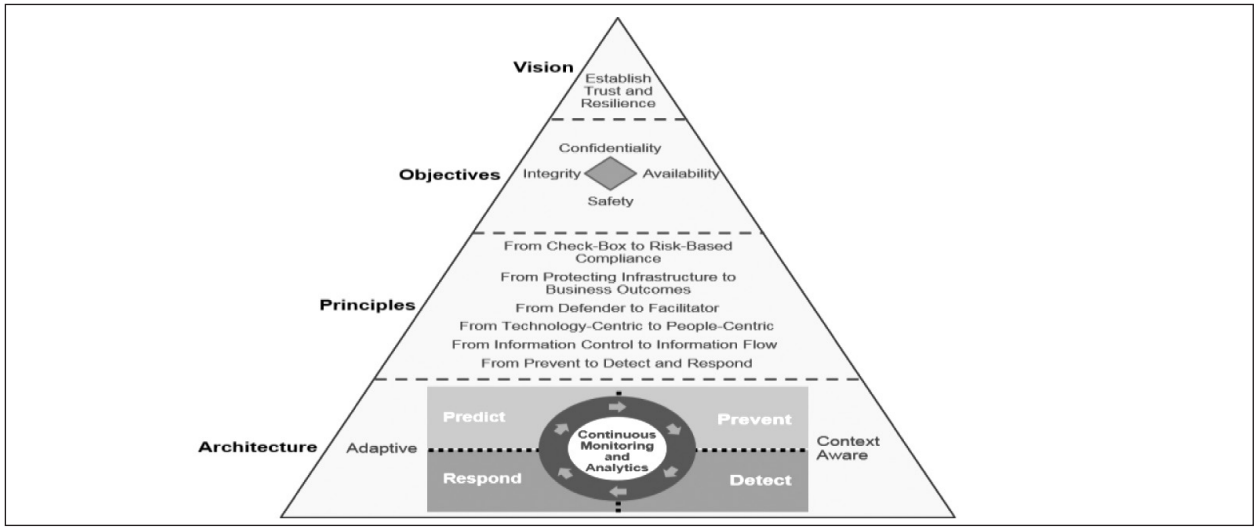
– همان‌طور که اســـتقلال کســـب و کار در پیاده‌سازی فناوری‌های جدید دیجیتال افزایش می‌یابد، سطح اختیارات سازمان فناوری اطلاعات مرکزی، نزول می‌کند.

– کاهـــش ناگهانـــی تعـــداد عناصر (مانند ســـامانه‌ها، دســـتگاه‌ها، داده‌ها و روابـــط پویا)، باعث بروز مســـائل مقیاس‌پذیری با بسیاری از راهکارهای سنتی کنترل امنیت می‌گردد.

این واقعیـــت، وضع موجود در مدیریـــت مخاطرات و امنیت اطلاعات را به چالش می‌کشـــد. بسیاری از روش‌ها و فناوری‌هـــا که تجارب مخاطـــره و امنیت بر مبنای آن‌ها بوده اســـت در مقیاس این واقعیت تازه نمی‌گنجند. رهبران مخاطرات فناوری اطلاعـــات و امنیت اطلاعات باید برنامه خود را برای تبدیل شـــدن به یک عامل توانمندسازی برای کســـب و کار دیجیتال به جای مانعی برای نوآوری، آن را ارزیابی کرده و متناســـباً تغییر شـــکل دهند [۶]. مؤسسه گارتنر چندین پژوهش در این حوزه انجام داده اســـت که توسط آن‌ها، تجارب امنیتی و مخاطره‌ای را با عصر کسب و کار دیجیتال متناســـب می‌سازد (شـــکل ۳) [۶]. البته این پژوهش‌ها جهت تکامل همچنان ادامه دارند.

نقطـــه آغازین برنامـــه مخاطره و امنیت، توســـعه یک دید متقاعدکننده اســـت که ســـایر بخش‌های کسب و کار بتوانند آن را درک کنند و مانند یک هدف برای فعالیت‌های طرح‌ریزی راهبـــردی عمل کند. معمولاً هـــدف یک برنامه امنیت اطلاعات یا برنامه مدیریت مخاطرات، ایجاد روشـــی

6- Mode 2 Projects



شکل ۳: مبانی مخاطره و امنیت در دنیای کسب و کار دیجیتال [۶]

مداوم، تکرارپذیر و بهبوددهنده برای طرح‌ریزی، ساخت و اجرای راهکارهای امنیتی است که با الزامات کسب و کار هم‌راستا باشد. بیشتر سازمان‌ها یک دید ابتدایی مانند ISMS را از استانداردها و چارچوب‌های موجود مانند ISO 27001 توسعه می‌دهند.

دید لازم برای مخاطره و امنیت در کسب و کار دیجیتال باید بر مبنای ایجاد یک زیست‌بوم باشد که اعتماد و تحمل‌پذیری را ممکن می‌سازد. این دید باید: ۱- افراد، فرآیندها و فناوری را تحمل‌پذیرتر نماید، ۲- آگاهی را در میان سودبران برای ایجاد اعتماد و تحمل‌پذیری افزایش دهد، ۳- راهبرد دونمایی فناوری اطلاعات را پشتیبانی کند، ۴- برای شرایط جدید و بی‌سابقه برنامه‌ریزی کند و ۵- به نیازهایی بپردازد که مربوط به حفاظت از دارایی‌هایی هست که فناوری اطلاعات دیگر مالک آن‌ها نیست و آن‌ها را کنترل نمی‌کند [۷].

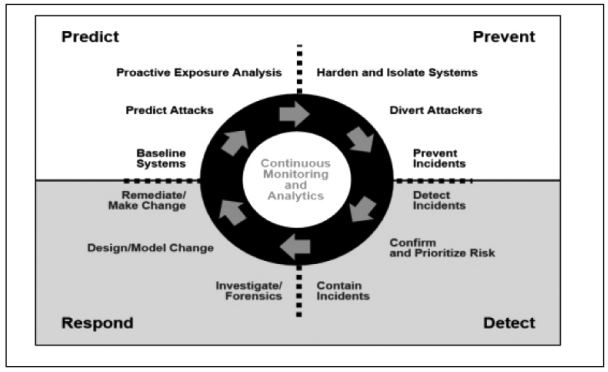
چنین محیط پویایی برای برای داشتن برنامه مخاطره و امنیت موفق، مستلزم پذیرش مجموعه‌ای جدید از اصول کلیدی است: ۱- متوقف کردن تمرکز بر روی انطباق موردی و انتقال به تصمیم‌گیری مبتنی بر مخاطره، ۲- متوقف کردن حفاظت منحصر به زیرساخت و آغاز پشتیبانی از خروجی‌های کسب و کار، ۳- متوقف کردن مدافع بودن و تبدیل به تسهیل‌کننده شدن، ۴- متوقف کردن تلاش برای کنترل اطلاعات و تشخیص نحوه جریان آن، ۵- پذیرش محدودیت‌های فناوری و فردمحور شدن و ۶- متوقف کردن تلاش برای حفاظت کامل از سازمان و سرمایه‌گذاری در تشخیص و پاسخ‌گویی [۶].

تا کنون اکثر محصولات امنیتی به طور سنتی بر روش‌های مسدودسازی و پیش‌گیری (مانند آنتی ویروس) و یا کنترل‌های مبتنی بر خط‌مشی (مانند بارو[۷]) برای مقابله با تهدیدات متمرکز بودند. با این وجود، پیش‌گیری کامل غیر ممکن است. حملات پیشرفته به سادگی از باروهایی که از روش‌های پیش‌گیری مبتنی بر امضا استفاده می‌کنند عبور می‌کند و در حال حاضر تمامی سازمان‌ها به طور مداوم خود را در معرض خطر می‌بینند. گارتنر بر این باور است که برای ایجاد یک معماری جامع و قابل تطبیق برای حفاظت امنیتی، ۱۲ قابلیت ضروری است تا توانایی مسدود کردن و جلوگیری از حملات و همچنین تشخیص و پاسخ‌گویی به آن‌ها نیز افزایش یابد (شکل ۴).

۲-۳-۲ مدیریت مخاطره و امنیت در فناوری اطلاعات دونمایی

مدیران ارشد امنیت اطلاعات و راهبران مدیریت مخاطره باید قابلیت‌های تیم خود را مجدداً برآورد کرده و تکمیل کنند تا اطمینان حاصل کنند که آن‌ها در زمان فعالیت

7- firewall



شکل۴: ۱۲ قابلیت حیاتی معماری امنیتی قابل تطبیق گارتنر [۶]

در رویکردهای چابک‌تر توسعه به عنوان بخشی از تغییر شکل دیجیتال، امنیت مناسب را نگهداری می‌کنند.

هنوز رهبران مدیریت امنیت و مخاطره در اغلب موارد، درگیر قدم‌های آغازین تبدیل به فناوری اطلاعات دونمایی نیستند و سپس برای گرفتن این پروژه‌ها شروع به کشمکش می‌کنند. تیم‌های امنیتی زیر فشار هستند، زیرا فناوری اطلاعات دونمایی در بسیاری از سازمان‌ها در حال به وقوع پیوستن است و هر کسی انتظار دارد که امنیت در هر دو نما به یک اندازه مهم باشد. برای موفقیت، رهبران مدیریت امنیت و مخاطره نیاز به تغییر طرز فکر، تعهد محکم و همکاری بین تیم‌ها دارند.

برای پایداری طولانی‌مدت فناوری اطلاعات دونمایی، مدیران ارشد امنیت اطلاعات باید نقشه راهی برای پشتیبانی از پروژه‌های نمای ۱ و نمای ۲ فراهم کنند. مؤسسه گارتنر پیش‌بینی می‌کند که در سال ۲۰۱۹، ۳۰٪ از مدیران ارشد امنیت اطلاعات، عملیات مدیریت مخاطره را در سازمان خواهند پذیرفت تا از فناوری اطلاعات دونمایی پشتیبانی کنند و نرخ موفقیت نمای ۲ را بهبود بخشند [۸].

همچنین مؤسسه گارنتر، یک طرح ۴- قدمی را برای کمک به مدیران ارشد امنیت اطلاعات طراحی کرده است تا بتوانند به این موفقیت دست یابند (شکل ۵) [۹]. البته اکثر قدم‌های این طرح باید هم‌زمان به وقوع بپیوندند و این‌گونه نخواهد بود که الزاماً این مراحل، به صورت متوالی انجام بپذیرند.

۲-٤ امنیت رایانه‌ای در ضلع جدید

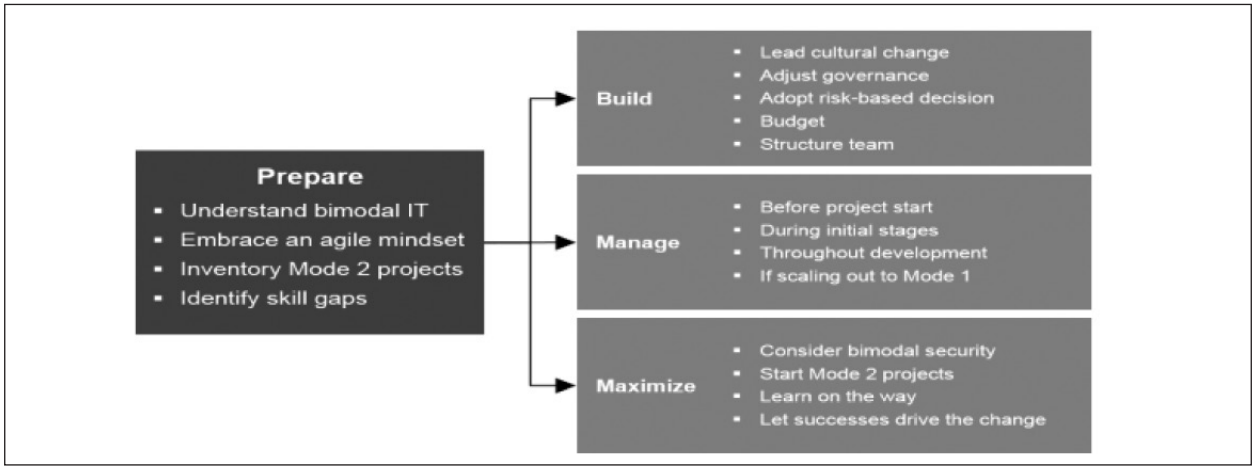
این بخش، اشتراک و شباهت بسیاری با بخش قبلی دارد. البته در این بخش مفاهیم بخش قبلی کاملاً شرح داده خواهند شد تا وضعیت امنیت رایانه‌ای در ضلع جدید و تغییرات لازم برای مدیریت موفقیت‌آمیز مخاطرات و امنیت اطلاعات مشخص گردند.

ضلع جدید، مرکز داده‌ها را فراتر و به سمت فناوری عملیاتی، ابر و نرم‌افزار به‌عنوان خدمت (SaaS) هدایت کرده است. سازمان‌ها نیاز دارند تا در مورد فناوری‌ها و دارایی‌هایی که دیگر مالک آن‌ها نیستند یا کنترلی روی آن‌ها ندارند به امنیت رایانه‌ای و مخاطرات آن‌ها بپردازند. فناوری اطلاعات در کسب و کار، حقیقتی در بیشتر شرکت‌های امروزی است و با نگرانی‌های مخاطره‌ای و امنیت رایانه‌ای، تعطیل نخواهد شد، بلکه باید پذیرفته و مدیریت شود تا سطح مناسبی از حفاظت را به ارمغان بیاورد [۱].

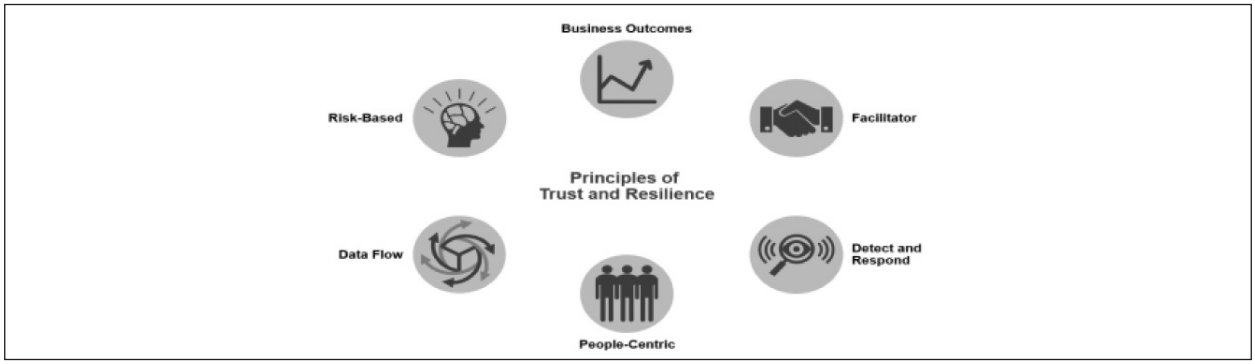
اینترنت اشیاء، یک حضور دیجیتال جامع ایجاد می‌کند که سازمان‌ها و اجتماع را به هم اتصال می‌دهد. بازیگران جدید آن شامل دانشمندان داده‌ها، عاملین خارجی جامعیت و نقاط پایانی مورد نظر هستند. تصمیم‌گیرندگان امنیتی باید اصول پایه مخاطره و تحمل‌پذیری را بپذیرند تا تغییرات را کنترل کنند [۱۰].

امن‌سازی اینترنت اشیاء شامل تغییری در طرز فکر در میان متخصصان فعلی امنیت اطلاعات است. تحول در نوآوری فناورانه علاوه بر این که مجوز دسترسی بی‌سابقه به داده‌ها را می‌دهد و اقدامات فیزیکی (خودکارسازی) را پایه‌گذاری می‌کند، موجب پیچیدگی سطوح و نیاز به هماهنگی الزامات می‌شود و در نتیجه باعث افزایش سطح تهدیدات در فناوری‌ها و فرآیندها می‌گردد.

با به کارگیری دستگاه‌های اینترنت اشیاء، یک حضور دیجیتال جامع در سرتاسر فرآیندها و عملیات کسب و کار ایجاد شده است. این حضور، بینشی در عملیات کسب و کار و خودکارسازی تولید برای تمام سازمان‌ها فراهم



شکل۵: ۴ قدم برای هم‌راستاسازی امنیت با فناوری اطلاعات دونمایی [۹]



شکل۶: اعتماد و تحمل‌پذیری در امنیت دیجیتال [۱۰]

نموده اســت. هم‌زمان با ورود این دستگاه‌ها، دانشمندان داده‌ها و عاملین جامعیــت، در مدیریت مخاطره ناآزموده هستند. این حضور، یک فرامجموعه[8] امنیت دیجیتال ایجاد می‌کند کــه در زمان ســاخت، پیکربندی، پیاده‌ســازی و عملیاتی‌سازی این دستگاه‌ها و کار با متخصصان جدید به دنبال به کارگیری اصول اساســی مخاطره و تحمل‌پذیری است [۱۰]. این اصول در شکل ۶ نشان داده شده‌اند.

امنیت دیجیتال، مفهوم بسط‌یافته امنیت رایانه‌ای فعلی است که توسط مخاطره و تحمل‌پذیری هدیت شده است تا از حضور جامع دیجیتال در کسب و کار، حاکمیت و اجتماع حفاظت کند. همان‌طور که در شــکل ۱ نشان داده شد، این امر مستلزم متخصصان امنیتی است تا ۶ اصل مهم را برای پرداختن بــه امنیت دیجیتال به طور موثر ایجاد کند. این ۶ اصل به شرح زیر هستند: ۱- خروجی‌های کسب و کار، ۲- تســهیل‌کننده، ۳- تشخیص و پاسخ‌گویی، ۴- فردمحوری، ۵- جریان داده‌ها و ۶- مبتنی بر مخاطره بودن [۱۰].

۲-۵ افراد و فرآیند: تغییر فرهنگی

هر رهبر کســب و کار و فنــاوری اطلاعات باید اخلاق دیجیتــال را اولویت‌بندی کند. نتایج اخلاقی ناخواســته در کســب و کار دیجیتال، چالشی برای تمامی صنایع است و راهنماهایی در حال به وجود آمدن است تا این‌که بتوان از این نتایج ناخواسته اجتناب کرد [۱۱].

اخلاق دیجیتال اغلب خود را به شکل دوراهی‌های مشکل نشان می‌دهد. حل این دوراهی‌ها بسیار مشکل است، با این وجود بیشــتر آن‌ها می‌توانند در زمینه‌های مشترکی جای گیرند. با استفاده از این زمینه‌های مشترک می‌توان ۳ نوع

8- Superset

را برای این دوراهی‌ها مشخص کرد [۱۲]:

– ایـــن در مقابـــل آن: اغلـــب می‌توانند با جســـتجوی روش‌هایـــی برای حـــذف محدودیتی که انتخـــاب را اجبار می‌کند، مورد مصالحه واقع شوند.

– تو در مقابل من: اغلب از طریق جستجوی هم‌راستایی و اصول بالاتر، حل می‌شوند.

– حال در مقابل آینده: مســـتلزم یـــک راهبرد مبتنی بر انتخاب و گزینه است [۱۳].

بسیاری از سازمان‌ها این دوراهی‌ها را تجربه می‌کنند و بسیاری از این دوراهی‌ها، عناصر مشترکی دارند. برای هر نوع از این دوراهی‌ها، مؤسسه گارتنر بررسی دقیقی در ۳ حوزه انجام داده و برای هر حوزه، راهنماهایی پیشنهاد کرده است [۱۲]:

– رفتار و ارتباط

– فرآیند و سازمان

– فناوری و داده‌ها

در ایـــن دوراهی‌ها معمـــولاً انجام یک انتخـــاب، ایجاد یک تعادل یا جســـتجوی یک توافق، بهترین راهکار نیست. بهترین راهکار برای حل این دوراهی‌ها، انتخاب یک فرآیند مصالحه‌گونه یا ترکیبی است که راه‌هایی را برای برآورده کردن الزامات هر دو راه نتیجـــه می‌دهد. این کار می‌تواند به چند روش انجام گیرد. بسیاری از دوراهی‌های اخلاقی که در این پژوهش‌های مؤسســـه گارتنر ذکر می‌شـــوند، دوگانه‌های اشتباهی هستند. برای مثال ارزش سهامداران و مشـــتریان متضاد نیســـتند، بلکه هر دو باید از کسب و کار بهتر، ســـود ببرند. همچنین حریم خصوصی و ارزش مشتریان نیز سناریوی دیگری است که اغلب به عنوان یک مورد قابل مصالحه در نظر گرفته می‌شـــود. می‌توان گفت که در واقع حریم خصوصی، یک پیش‌شـــرط برای ارزش مشتریان سالم است.

۲-۵-۱ دوراهی‌های این در مقابل آن

این دوراهی‌ها، ما را در یک موقعیت مشکل قرار می‌دهند که باید بین دو پدیده خارجی که به وضوح متضاد هستند، یکی را انتخاب کنیم. البته همان‌طور که گفته شد این پدیده‌ها الزاماً متضاد نیستند. این پدیده‌های متضاد می‌توانند افراد، کســـب و کار، نظرات یا مفاهیم باشند. انواع این دوراهی‌ها به شرح زیر می‌باشند:

– دسترسی در مقابل حریم خصوصی

– شخصی‌سازی در مقابل حریم خصوصی

– امنیت در مقابل حریم خصوصی

– ارزش مشتری در مقابل حریم خصوصی

– هم‌راستایی در مقابل چابکی

– ایمنی در مقابل آزادی

– تغییر در مقابل پذیرش

– لذت مشتری در مقابل اراده آزاد

– سهولت استفاده در مقابل تناسب

– سهولت استفاده در مقابل وابستگی به فناوری

۲-۵-۲ دوراهی‌های تو در مقابل من

ایـــن دوراهی‌ها، تقابـــل الزامات ســـودبران مختلف با بخش‌های درگیر (معمولاً خود ما) است. انواع این دوراهی‌ها به شرح زیر می‌باشند:

– اجبار قانونی در مقابل حریم خصوصی

– درآمد در مقابل حریم خصوصی

– نیاز به تعداد بالا در مقابل نیاز به تعداد کم

– ارزش کسب و کار در مقابل ارزش سودبران

– دید در مقابل حریم خصوصی

– ارزش کسب و کار در مقابل ارزش اجتماعی

– شفافیت در مقابل حریم خصوصی

۲-۵-۳ دوراهی‌های حال در مقابل آینده

ایـــن دوراهی‌ها، تقابل مســـائل کوتاه‌مدت با مســـائل بلندمدت است. بسیاری از افراد از تمایلات کوتاه‌مدت رنج می‌برند و طرفدار مزایای فوری مخاطرات بلندمدت هستند. انواع این دوراهی‌ها به شرح زیر هستند:

– گزینه‌های آینده در مقابل استفاده مناسب از داده‌ها

– کنار گذاشتن در مقابل دقیق انجام دادن

– مزایای کوتاه‌مدت در مقابل مخاطرات بلندمدت

۳. نتیجه‌گیری

در این پژوهش بـــه مرور عوامل امنیت رایانه‌ای موفق در کسب و کار دیجیتال پرداختیم. پایه مفهوم کسب و کار دیجیتال، امنیت رایانه‌ای موفق اســـت. مؤسسه گارتنر در این حوزه پژوهش‌های بسیار مهمی انجام داده است که به بررسی برخی از آن‌ها پرداختیم. در بررسی‌های انجام‌گرفته مشخص شد که رهبری و حاکمیت، اولین و مهم‌ترین عامل موفقیت امنیت رایانه‌ای در این حوزه اســـت، زیرا با توجه بـــه تغییرات فضای کاری و مخاطـــرات و انتظارات جدید، رهبران و مدیران امنیتی نیز باید توانایی‌های جدیدی داشته باشند تا بتوانند این مخاطرات و انتظارات را مدیریت کنند. دیگـــر عامل مهم در این حوزه، تهدیدات روزافزون و جدید آن است که اشاره کردیم برای مدیریت آن‌ها باید تمهیدات جدیدی اندیشیده شـــود. همچنین موضوع امنیت رایانه‌ای در فناوری اطلاعات دونمایی موضوع بســـیار مهمی است که با توجه به تفـــاوت پروژه‌های این محیط با محیط‌های قبلـــی کســـب و کار، نیازمنـــد رویکردهای جدیـــدی برای مدیریت امنیت رایانه‌ای است. در این محیط بیشتر اطلاعات و عملیات به ســـمت نهادهـــای خارجی ماننـــد ابر هدایت می‌شوند و مدیریت امنیت این موضوع، چالشی بسیار مهم برای کســـب و کار دیجیتال است. در نهایت تغییر فرهنگی، آخرین عاملی بود که به بررسی آن پرداختیم و اهمیت آن را در کســـب و کار دیجیتال نشـــان دادیم و مشخص شد با اتخاذ راهکارهای مصالحه‌گونه و انتخاب‌های مناســـب می‌توان بسیاری از چالش‌ها و مشکلات آن را برطرف کرد. بنابراین جایگاه امنیت رایانه‌ای در کســـب و کار دیجیتال، جایگاهی بنیادین اســـت و با توجه به عوامل معرفی‌شـــده و مدیریـــت آن‌ها می‌توان کســـب و کاری موفق در دنیای دیجیتال داشت.

منابع

[1] Proctor P. E., Wagner R., “Special Report: Cybersecurity at the Speed of Digital Business”, Gartner, 2016.

[2] Joel B., Buckalew L., Loucks J., Moriarty R., O’Connell K., Riegel M., “Cybersecurity as a Growth Advantage”, Cisco, 2016.

[3] Pettey C., Van der Meulen R., “Gartner Says By 2020, 60 Percent of Digital Businesses Will Suffer Major Service Failures Due to the Inability of IT Security Teams to Manage Digital Risk”, http://www.gartner.com/newsroom/id/3337617, 2016.

[4] Perkins E., Byrnes F. C., “Cybersecurity Scenario 2020 Phase 2: Guardians for Big Change”, Gartner, 2015.

[5] Woods V., “Gartner Says Cybersecurity Professionals Are the New Guardians of Digital Change”, http://www.gartner.com/newsroom/id/3144319, 2016.

[6] Scholtz T., “Managing Risk and Security at the Speed of Digital Business”, Gartner, 2016.

[7] Pettey C.,“Security at the Speed of Digital Business”,http://www.gartner.com/smarterwithgartner/security-at-the-speed-of-digital-business, 2016.

[8] Wagner R., Deshpande S., D’Hoinne J., Young G., Proctor P. E., “Predicts 2016: Threat and Vulnerability Management”, Gartner, 2015.

[9] D’Hoinne J., Proctor P. E., “The Four Steps to Manage Risk and Security in Bimodal IT”, Gartner, 2016.

[10] Perkins E., “Securing the Internet of Things”, Gartner, 2016.

[11] Buytendijk F., Vashisth S., Duncan A. D., Moran M. P., “Kick-Start the Conversation on Digital Ethics”, Gartner, 2016.

[12] Buytendijk F., “Digital Ethics, or How to Not Mess Up With Technology”, Gartner, 2014.

[13] Buytendijk F., Sommer D., Oestreich T. W., “Maverick Research: We Analyze Too Much, and Synthesize Too Little”, Gartner, 2014.