جلسه هفتم

تحصیل برنامه ها و زیرساخت فناوری اطلاعات

نکته پایانی مهم در ارتباط با فصل ۱۴ این است که با فرآیندهای سنتی شرکتها ،با دستورالعمل ها، آیین نامه ها و بخش نامه های رایج برای مکانیزم شرکت ها ، نمیشود شرایط رو توسعه داد و این نیازمند این است که یک قسمتی یا بخشی و یا مجموعه زیادی از این دستورالعمل ها، بخش نامه ها، آیین نامه ها و فرآیند ها عوض شود.

اول اینکه تغییر دادنش در عمل اصلا کار آسانی نیست به هر حال سازمانها یا مدیران سازمان نسبت به این قضیه مقاومت نشان میدهند و گاهی اوقات هم ممکنه این جمله رو زیاد بشنویم که تغییر این بخشها و این آیین نامه اصلا از حدود اختیارات ما خارج است و امکانش نیست و این مشکل بزرگ در توسعه شبکه است.کتاب در قسمت پایانی بیان می کند که ایجاد تغییر در زیر ساخت و توسعه شبکه ها در بیشتر مواقع احتیاج به مهندسی مجدد فرآیند ها و معیارهای بزرگ و تغییرات عظیم در فرایندها و روشهای کار داره که این معظل مهمی است که به سادگی نمیشه این قضیه رو حل کرد و گاهی اوقات چالشها و مشکلات بسیار زیادی رو در توسعه زیر ساخت برای پیمانکاران پروژه های سیستم های اطلاعاتی بوجود می آورد. یک بحث دیگه که در انتهای فصل ۱۴ مطرح شده، بحث های رفتاری و مقاومت های دستگاه کارکنان ، تصمیم گیرندگان ، مهندسین و مدیران شرکت ها نسبت به این تغییر است. سازمان یا شرکت نسبت به تغییرات مقاومت نشون میدن.

گاهی اوقات با جزیی ترین طرح ها با دلایل کافی با جزییات زیاد هم اگر براشون استدلال میشه که این فرایند یا این بخش نامه به این شکل باعث مثلا افزایش قیمت تمام شده ی فرایندها میشه یا باعث افزایش زمان انجام فرایند ها میشه. باز هم میگن عملا نمیتوانیم کاری کنیم این نیاز به تصمیمات بیشتر یا مطالعات بیشتر یا تصمیم گیری از حوزه های بالاتر از سازمان ،که این یک مشکل بزرگ است که در عمل بسیاری از مجریان سیستم های اطلاعاتی را با مشکل روبرو میکند. البته در عمل بخشی از این مقاومتها به حق است ،یعنی واقعا از حیطه ی

وظائف افراد خارج است، اما یه قسمتی که اون خیلی خطرناک است جنبه ی مقاومت- RESISTANCE – است که افراد نشان می دهند.

کلا انسانها بنده ی عادت هاشون هستند، دوست دارند همون روشهایی که در زندگی شان دارند و اجرا می کنند ، ادامه پیدا کند. در محیط کاری هم افراد هر چه سابقه ی کاریشون بیشتر میشه مقاومتشون در برابر تغییر بیشتر میشه، به همین دلیل در قسمت آخر فصل ۱۴ بحث زیر ساختی ،همه ی مسایل زیر ساخت، بحث های بودجه، کمبود منابع ویا بی میلی دولت نیست، یه بحث مهم این که فرایندهای شرکتها باید عوض بشه و برای تغییر این فرایندها به یک سری راهکارها و برگزاری جلسات برای توجیه ،اون هم معلوم نیست مدیران شرکت فعلی ما در اختیاراتشون نباشه یا مقاومت کنند، در اداره مرکزی مطرح بشه ،باز هم توسعه زیر ساخت را مشکل میکند.

فصل ۱۵

مدیریت منابع اطلاعات و امنیت

در این فصل بحث مدیریت منابع اطلاعات و امنیت مطرح است. در ابتدای این فصل مطرح شده که نگرش شرکتها به بحث سیستم های اطلاعاتی ممکن است بسیار سطحی باشد تا یک نگرش کلان و جامع.

در ابتدا توسعه ی سیستم های اطلاعاتی ممکن است به عهده ی یک کمیته باشد ، که این کمیته رشد کند و تبدیل به یک شورای دائمی بشود. بعد این رشد ادامه پیدا کند و تبدیل به اداره و مدیریت در یک شرکت بشود ، اگر خیلی رشد کند و خیلی بزرگ بشود میتواند تبدیل به یک معاونت در شرکت بشود . بنابراین گذر از توسعه این چارت سازمانی از یک گذر ساده به یک گذر عظیم است که بستگی به نوع فرایندها ، بستگی به سطح توسعه شبکه در شرکت دارد که این می تواند از یک حداقل تا یک حداکثر ، از یک کمیته ی موقت تا یک معاونت بزرگ در یک شرکت بشود و کار کند، اسمش توی شرکتهای ما خیلی گوناگون است ، ممکن است بگویند مدیریت شبکه یا مدیریت فناوری اطلاعات.

در برخی از شرکتها می گویند فناوری اطلاعات ، حالا اسمش به هر شکلی باشد این نیازمند یک نگرش عظیم در چارت سازمانی شرکت هست. بحثی که در فصل ۱۵ شروع می شود این است که معمولا در فرایندهای توسعه اطلاعاتی حدود یک چهارم (۲۵ درصد) ارزش کل قرارداد باید صرف نگهداری و پشتیبانی شبکه شود. حالا اگر اون ۲۵ درصد رو به عنوان کل در نظر بگیریم ،سه چهارم(۷۵ درصد) صرف کنترل امنیت وتحقیق های امنیتی درشبکه می شود. مساله مهم که امروزه شاید زیاد در شرکتها گزارش میکنند بحث حمله به زیر ساختهای شرکتها توسط کاربران غیر مجاز است که ما می گوییم هک کردن.

اینها همانطور که اشاره کردم گاهی اوقات ممکن است شرکتهای بزرگ مثل یاهو را هم متوقف کنند، به عنوان مثال (تهدید امنیتی): فرض کنید که شما تلفن روابط عمومی یک سازمان رو از کار بندازید، اگه شما سیستمی داشته باشید که در آن واحد هزار نفر شروع کنند به تلفن کردن به این شرکت ، این خود به خود باعث می شود که ترافیک ایجاد شود. عملا یک کاربر اصلی و کاربران دیگه ای که می خواستند انجام بشود اون خط براشون اشغال میشه.

این فکر هایی که ایجاد می شود یا تحقیقات امنیتی که باعث متوقف کردنش می شود، باید یک تیم های زیادی رو استخدام کنیم، دستمزد بالایی در خواست داده بشه که مساله این مشکلات شناسایی و رفع کنند و جلوی تکرار این تهدیدات امنیتی رو در آینده بگیرند. به هر حال تهدیدهای امنیتی و بحث امنیتی که موضوع فصل ۱۵ است یه بحث مفصل در این کتاب دارد ، که شرکتها و گاهی اوقات هزینه هایی که برای کنترل این تهدیدات و پیشگیری این تهدیدها و دسترسی های غیر مجاز متقبل می شوند امروزه هزینه های سنگینی هست که در فصل های دیگه اشاره می کنیم شاید یکی از مهمترین روش های کنترل این تهدیدهای شبکه ، تدوین یک سری عوامل و مقررات حقوقی به عنوان کنترل جرائم سایبری می باشد.

در خیلی از کشورهای دنیا مثل اتحادیه اروپا یا خوده امریکا و کانادا ۳۰ سال هست که این قوانین و مقررات وجود دارند، از دهه ۸۰ میلادی به بعد. که دادستانهای فعال، پلیس های سایبری و فعال هستند و شرکتها شکایت می کنند که بتوانند در مرجع قضایی باید ادله مناسب و پشتیبانی قانونی متناسب با خسارت که به شبکه هاشون وارد

کرده بتوانند شکایت هاشون را دنبال کنند و بتونند ادعای خسارت کنند. در ایران ما در این زمینه در حال هشیار هستیم شاید دلیلش این باشه که سواد اطلاعاتی افراد جامعه ما نسبت به شبکه، درصدش نسبت به کل جمعیت ۷۸ میلیون زیاد نیست ولی در خیلی از کشورها مثل چین، هند، هنگ کنگ، جرائم اینترنتی زیاد هست ، اینه که جمعیت زیادی از مردم حالا دانشگاهی یا غیر دانشگاهی نسبت به سواد شبکه اگاهی های زیادی دارند. حالا این بد هم نیست مثلا می گوییم که خب باشه آگاهی ندهیم ، نیازی نیست که همه افراد مطلع باشند . افراد یاد میگیرند این کار رو، راهش این نیست که آگاهی ندیم. به نظر میرسد راهش این است که برای کنترل باید نظامهای حقوقی-قانونی و دادستانهای فعال در این زمینه وجود داشته باشند. درست مثل این که ما بگوییم مثلا مردم از خودرو استفاده نکنند چون مرتکب تخلف می شوند. راهش این است که با استفاده از خودرو، جاده ها ، بزرگ راه ها بیشتر بشه اما نظارت و کنترل دقیق تری انجام بشه. اما متاسفانه توی ایران در این زمینه یه مقدار مسیر رو اشتباه می رویم. به همین دلیل است که سواد اطلاعاتی افراد جامعه ما و توسعه خدمات الکترونیک برای شهروندان الکترونیک در اقتصاد الکترونیک و بازرگانی الکترونیک رشد نکرده .شاید اگر در آینده این رشد کند و اگاهی و سواد طبقه عام جامعه رشد کند شاید ما از کشورهایی باشیم که از جرائم اینترنتی مصداق داشته باشیم. به هر حال توی این زمینه باید بیشتر کار بشود و این پروژه ای است که حالا بحث امنیت در فصل ۱۶ کتاب در جلسات اینده بیشتر گفته می شود.