جلسه هشتم

مدیریت منابع اطلاعاتی و امنیت

بحث هایی که در این فصل دنبال میشه اول اینکه بحث جایگاه سازمانی اداره فن آوری اطلاعات ، اداره خدمات ماشینی یا دپارتمان فن آوری اطلاعات در شرکتها و سازمان ها ست.

در شرکتهای مختلف یا سازمان های گوناگون به اسم های مختلف این دپارتمان توی چارت سازمانی نامگذاری میشه اما اگر یک سلسله مراتب بخواد رعایت بشه به موزاتی که استفاده از شبکه یا سیستم اطلاعات در شرکت یا سازمان بیشتر بشه جایگاه سازمانی واحد فن آوری اطلاعات هم بزرگتر میشه و نقشش و نیروهاش و level سازمانیش افزایش پیدا میکنه ترتیبش به این صورت هست که در اوایل ، در سالهای اول بهره برداری معمولا یه **کمیته فن آوری اطلاعات** در شرکت ها شکل میگیره به موازاتی که این کمیته فعالیتها و وظایفش بیشتر میشه تبدیل به یک **شورای فن آوری اطلاعات** میشه که خوب معمولا در مراحل اولیه طرح ریزی شبکه تمام مراحل زیر نظر این شورا اتفاق میفته . بعد از نصب و راه اندازی شبکه واحد فن آوری اطلاعات میتونه از یک شورا به **یک اداره** تبدیل میشه ، اداره فن آوری اطلاعات که خوب دارای یک مدیریت مستقل به نام مدیر خدمات ماشینی یا **مدیریت فن آوری اطلاعات** هست . معمولا در فاصله بین ۳ تا ۷ سال بهره برداری جایگاه فن آوری اطلاعات در همین قالب می تونه باقی بمونه شاید هم بیشتر اما برخی از شرکتها هستند که شبکه هاشون بعد از یک دوره ۳ تا ۷ ساله خیلی رشد میکنه و این عظیم میشه و به نمایندگی های بیشتر و شعبات بیشتر به پراکندگی جغرافیایی بیشتر و محصولات و خدمات و بازارهای منطقه ای و فرا منطقه ای بیشتر در این شرایط خاص هست که ما در چارت سازمانی مان یک تحول خواهیم داشت و مدیریت فناوری اطلاعات تبدیل به یک معاونت میشه ، **معاونت فن آوری اطلاعات** . بنابر این عالی ترین سطحی که برای اداره خدمات ماشینی یا فن آوری اطلاعات یا مدیریت شبکه وجود داره این است که این در چارت سازمانی شرکت اینقدر بزرگ بشه و که به

عنوان یک معاونت مستقل تحت عنوان معاونت خدمات ماشینی یا معاونت شبکه یا معاونت بهره برداری یا معاونت فن آوری اطلاعات ازش اسم برده بشه . بنابر این در یک سیر تاریخی از یک کارگروه و یک شورا میتونه رشد بکنه ، بزرگ بشه وبه یک مدیریت و در نهایت معاونت مستقل در سازمان تبدیل بشه.

نکته دیگه ای که در این فصل بهش اشاره شده این است که به موازات افزایش جایگاه واحد فن آوری اطلاعات در این سلسله مراتب و چیدمان شغلی ، مشکلات و چالشهای این اداره روز به روز بیشتر خواهد شد شاید متداول ترین مشکلی که این واحد با بقیه بخش های شرکت می تونه داشته باشه بحث زبان کاریشون باشه . معمولا واحد فن آوری اطلاعات و خدمات شبکه ای دارای یک زبان فنی هستند زبان کامپیوتر و نیروهایی که درش مشغول به کار هستند دارای همین زبان هستند ، اما بخش های دیگر سازمان ، کارکنان و مدیران و حوزه های دیگر سازمان خیلی ممکنه زبان فنی شان به این نزدیک نباشه و این باعث یک شکاف ، باعث یک تعارض و گاهی اوقات باعث یک دو دستگی بین نیرو های فنآوری اطلاعات شرکت با بقیه کارکنان می شه. این یک مسئله هست که توی همه شرکتها هم وجود داره و یک جور دو دستگی یا نگرش گروههای فنی حوزه IT با بقیه نیرو های شرکت همیشه وجود داشته باشه تا وقتی چالشهای دیگری نیز میتونه اتفاق بیفته.

امنیت

نکته دیگری که وجود داره امنیت تا به امروز چه در کشور ما چه در کشور های دیگر هیچ کشوری نبوده که از بحث های امنیت خسارت ندیده باشه . بنابر این یک معضل بزرگ شرکتها و سازمان ها نحوه نظارت بر بهره برداری و استفاده از شبکه هست . بحث امنیت امروزه یکی از بحث های فراگیر برای همه شرکت ها و بیشتر یک دغدغه بزرگ است و چالش فکری هست و همیشه شرکتها رو با یک دلواپسی و با یک نگرانی از سرقت اطلاعات میشه این و باهاش دنبال کرد. شاید همینطور که کتاب مثال زده و دوستان اشاره کردن خیلی وقتها در روزنامه ها و خبرگزاریها گزارش های خیلی عجیب مطالعه میکنیم که یک فرد با دانش کم دست به سرقت زده که این دیگه شناخته شده هست و تقریبا عادی شده وقتی آدم این چیزارو میشنوه و یک کسی داره یک کارهایی رو انجام میده بنابر این بحث سرقت و تخریب شبکه ها امروزه یک بحث بزرگ هست . بحث امنیت در شبکه ها معمولا به ۲

شکل دنبال میشه یعنی ما همیشه ۲ نوع تخریب شبکه همیشه می تونیم داشته باشیم :

نوع اولش دسترسی غیر مجاز هست . در این نوع نفوذگر یا هکری که این کار را انجام میده حالا می تونه یک فرد یا یک گروه باشه تمایل داره که اطلاعات یک شبکه رو سرقت کنه و فایلاشو کپی کنه این یه نوع هست.

نوع دومش که از نوع اول خطرناک تر هست انگیزه نفوذگر سرقت دیتا نیست **تخریب زیر ساخت شبکه** هست .

بنابر این ۲ نوع نفوذ خواهیم داشت : **یکی نفوذ و انگیزه دسترسی غیر مجاز به داده های شبکه و نوع دوم انگیزه تخریب ارکان شبکه هست** . برای هر دو نوعش معمولا یک سری تکنولوژی ها ، روش ها و قواعدی وجود داره ولی معمولا سرمایه گذاری که بر روی این تکنولوژی ها میشه دارای یک قاعده مشخص هست . اول اینکه در سالهای اولیه بهره برداری از شبکه یعنی سال اول تا حداکثر سال سوم باید حدود ۱۵ تا ۲۵ درصد از بودجه شرکت صرف طراحی و نصب شبکه میکنه صرف هزینه های نگهداری و تامین امنیت شبکه شود .حالا اگه این پول در ۲۵ درصد کل را در نظر بگیریم حداقل ۴۰ درصدش صرف خرید تجهیزات و تکنولوژی و امکانات و خدمات و وسایل و لوازمی بشه که این امنیت رو باید فراهم بکنه در بخش های بعدی کتاب انواع روش های تکنولوژی هایی که برای این قضیه وجود داره خیلی هایش هم شما در کتاب میبینید مثال میزنیم حالا از اسکن کردن چهره افراد ، اسکن کردن اثر انگشت ، اسکن کردن شبکیه و عنبیه چشم افراد تا تکنولوژی هایی در دنیا معرفی میشه اما اینها موضوع نیست. موضوع این است که بحث بزرگی که وجود داره این است که سرمایه گزاری و خرید تکنولوژی برای تامین امنیت شبکه ها چند تا مشکل داره یعنی به این سادگی هم نیست که بگیم آقا فلان چیز را در بازار جست و جو کنیم این تکنولوژی ها رو بیاریم و به قول معروف دغدغمون رو کم کنیم ، خیال خودمون رو راحت کنیم یه مشکل که داره این هست که یعنی این امنیت میشه اینها خیلی راه کار نیست مسایل دیگه ای تو کار هست . اولین مشکلی که دارد این هست که **سرمایه گزاری روی این تکنولوژی ها هیچ ارزش افزوده** ای ایجاد نمیکنه درست مثل اینکه شما دیوار یک خونه رو ببرید بالا متراژ و مساحت ش چیزی

اضافه نمیشه این یه مسئله هست . بنابر این سرمایه گزاری روی تکنولوژی امنیت شبکه، ارزش افزوده ایجاد نمیکنه .

نکته دومش این هست که هر چقدر شبکه ای این تکنولوژی ها رو بیشتر روش سوار بکنیم مشکل بزرگی که براش پیش میاد کند شدن سرعت جریان داده و پردازش دیتا هست و این باعث میشه که خود به خود کندی ها و از کار افتادگی ها و هزینه رو افزایش بده . بنا بر این بی محابا نمیشه این تکنولوژی ها رو فورا تهیه کنیم فورا نصب کنیم فورا بگیم مشکل حل شد.

بحث سومی که وجود داره علاوه بر این در مورد این هست که روز به روز روش های نفوذ به شبکه ها متنوع تر میشه و این تکنولوژی ها دائما عوض میشه . بنا بر این باز هم به این شکل دنبال میشه ما باید هر روز ، هر سال در بودجه سالانه کشور مبلغ هنگفتی رو صرف این قضیه می کنیم . هیچ راهی نیست که امنیت شبکه رشد بکنه و یا برای چند سال این مشکل برطرف بشه باز می توان به روش های گوناگون ممکنه این اتفاق بیفته . در مجامع جهانی و کشور های مختلف دنیا یک مشکل ایجاد شده و اون هم این هست که به موازات افزایش زیرساخت افزایش سرعت اینترنت افزایش تعداد کاربران اینترنت یا تعداد افرادی که در شبکه ها حضور دارن این دو شاخص هست که میشه کشورها رو باهاش رتبه بندی کرد. امروز در مورد یک شاخص پهنای باند رتبه بندی هایی اتفاق افتاده که در آن کره جنوبی سر آمد هست یعنی بالاترین سرعت اینترنتی که وجود داره مربوط به کره جنوبی هست باپهنای باند ۲۴ شاید هم ۲۵ ، بعدش پهنای باند میاد روی ۱۰ تا ۱۲ آمریکا ، کانادا با یک اختلاف بزرگ و نصف میشه و در خیلی از کشورها اینترنت ضعیف میشه توی رتبه بندی که سال ۲۰۱۴ اتفاق افتاده کشور ما توی ۳۰ تا رتبه اول قرار داره .

این شاخصه خوب افزایش این زیر ساخت خیلی فرصتها ی تجاری زیادی برای شرکتها ایجاد کرده اما به موازات افزایش این زیر ساخت ها در همین کشور ها آمار جرائم ، آمار سوء قصد شبکه ها ، تخریب یا اصطلاحا نفوذ هک کردن شبکه ها در این کشور ها زیاد تر شده بنابر این یک قاعده وجود داره که هرچقدر زیر ساخت وجود داشته باشه احتمال تخریب و پایین آمدن سطح امنیت هم بیشتر میشه شاخص دیگه ای که وجود داره **شاخص**

بارگذاری اطلاعات هست که کشورها رو باهاش میسنجن که شما بهش آپلود میگید . در آپلود یا شاخص بارگذاری امسال دانمارک رتبه اول رو داره بعدش هامبورگ و این هم یک شاخص دیگه هست که می تونه شدیدا روی جرائم اینترنتی مؤثر باشه . گاهی اوقات هم همان طور که اشاره کردن نفوذگر یا هکر به دنبال برداشت اطلاعات نیست به دنبال سرقت فایل های اطلاعات شرکت ها و افراد نیست ، به دنبال این هست که فایل یا آرشیو شرکت رو دستکاری کنه و داده های غیر واقعی و داده های نادرست در شرکت بارگذاری یا آپلود اتفاق بیفته اینجا سرعت زیر ساخت ها خیلی نمیتونه بهش کمک کنه بنابراین به دلیل بحث های امنیت و کنترل این جرائم شرکت ها در سطح کلانش دولتها خیلی تمایل چندانی به افزایش زیر ساخت ها به صورت بی محابا به رتبه بالا رسیدن ندارند ، چرا؟ چون که این مسئله ، مشکلات عظیم تری به وجود میاره مثلا آمریکا سرعت اینترنتش رو از ۱۲-۵/۱۱ بیشتر نمیکنه بحث های کنترل کردنش خیلی بیشتر بشه ، کنترل کردن این قضیه مشکلات دیگه ای داره در داخل خود کشور ها امروزه به جایی رسیدیم که دولتها سعی می کنن از اموال شرکتهایی که هست کنترل بکنن ، برای این قضیه شاید شما شنیده باشید اکثر دولتها چیزی دارن به نام ارتش سایبری که این وظیفش حفاظت از زیر ساخت های عمومی در کشور هست که نفوذ چه در داخل کشور باشه چه در خارج کشور حفاظتش باید کنترل شده باشه یک نفوذ بی محابا به زیر ساخت میتونه سالها دستاورد رو از بین ببره ، سالها حفاظت و کنترل رو ضعیف بکنه.

شما مثلا ببینید ما شاید بالا ترین تجربه و تلخ ترین تجربه ای که در زمینه حالا زیر ساختی داریم در سطح ملی در کشور خودمون این چند سال اخیر شاید شما اسمش رو شنیده باشید اکستاکس نت هست که این اصولا یک زیر ساخت عظیمی از سازه ملی ما رو از بین برده یا متوقف کرده ، باید سالها روش کار بشه شاید لازم باشه دوباره سرمایه گزاری بشه و دوباره ساخته بشه ، شبکه های برخی از سازمان های دولتی ابسلوت کنه مجددا طراحی و نصب بشه یعنی گاهی اوقات تخریب به حدی هست که اصلا اصلاح کردنش مقرون به صرفه نیست بهتره که شبکه مجددا باز طراحی و نصب بشه و روشهایی به این شکلش حل بشه در داخل کشور ما الان ما قرارداد های سایبریمون خیلی فعاله البته بیشتر پدافندیمون هست اما برای مردم ما شناخته شده نیست بیشتر کارش حفاظت

از کشور است.

خیلی ها تلاش کردند که به شرکت های دولتی ما صدمه وارد بکنند و انبوه زیادی از کالاها و خدمات مختل بشه شاید اعتبارش کم بشه شاید گزارش هایی که این شرکتها ارائه می کنن داده هاش دستکاری شده باشه اصلا مبنای مناسبی برای تصمیم گیری براشون موجود نباشه .

به همین دلیل هست که بحث های امنیت و شبکه بحث های بسیار مهمی هست که موضوع این فصل از کتاب هست . قسمتهای بعدی این کتاب انواع تکنولوژی ها و روش ها و انواع حالا نفوذها رو بررسی میکنه البته یک نکته ای رو من خدمتتون بگم در هر کشوری که مردم ، تعداد کاربران شبکه ها شون یا تعداد افرادی که شناخت پیدا می کنن به مفهوم شبکه ، خدمات الکترونیکی ، آگاهی ؛ تجربه ، دانش ، شناخت و سواد مردم بدست میارن و این جمعیت بیشترمیشه و این چیز بدی نیست نباید بهشون بگیم این کار را نکن چیزی بلد بشن نه این درست نیست راهش این است که در خیلی از کشور های دنیا تجربه یا استراتژی که دنبال شده این هست که دو تا راهکار باید دنبال بشه. اول حتما لازمه یک سری قوانین و مقررات حقوقی و کیفری قوی در کشور وضع بشه و جرائم شبکه یک جرائم کیفری براش تعریف بشه. حالا در کتاب دنبال میشه در فصل های بعد .

و در خیلی از کشور ها داد ستانها و بازرسی ها و مراجه قانونی و قضایی زیادی هست که تخصصشون جرائم شبکه هست و این افراد کنترل میکنن خوب یه نوع سرقته دیگه و با سرقت از مغازه و خانه افراد فرقی نمیکنه این هم یک نوع سرقته چون شبکه روی اموال و دارایی شرکت هست سوء استفاده از اموال افراد بدون اطلاعشون یک جرمه دیگه و یک تخلف .این یک راهش ، راه دومش و اصلی ترش افزایش آگاهی و فرهنگ عمومی افراد نسبت به این قضیه هست . به روشهای گوناگون میشه کارکنان مخصوصا کارکنان شرکت یا مشتریان کاربران شرکت که از خدمات شبکه استفاده میکنن این افراد را مطلع کرد ، آگاه کرد که به چه روشهایی امکان سوء استفاده نفوذ و تخریب و سرقت داده هاشون در شبکه ممکنه اتفاق بیفته شرکت فقط نباید نگاهشون روی محیط داخل باشه ما فقط شبکه رو توسعه میدهیم هر بلایی سر مشتریامون میاد به خودشون مربوطه یکی اومد حسابشو خالی کرد یوزر و پس وردشون رو برد. باید خودشون هواسشون باشه . نه اینجوری نیست شرکتها باید در این زمینه

مسئولیت پذیری اجتماعی بیشتری بپذیرفتن مشتریان رو آموزش بدن حالا حتما نباید آموزش هایی نمیخواد حضوری باشه میتونه سایت الکترونیک باشه فایلهایی در سایتاشون قرار بدن انواع روش های اطلاعات رو بگن و ابنهارو شما کنترل کنید و غیره

حتما نیازی نیست همه مشتریان رو جمع کنیم توی سالن و آموزششون بدیم در بصورت الکترونیک دائم این دستور العمل ها رو آپدیت کنیم و توی سایت شرکتها بذاریم آموزش بدیم افراد و اینها هم باعث میشه تا حدودی بحث های امنیت جرائم ، سرقت و سوء استفاده از حالا جرائم اینترنتی و شبکه ها کاهش پیدا کنه

بحث امنیت موضوع خیلی مهمی هست سالها هست که در روزنامه ها جرائم گزارش های عجیب و غریبی نشون میدن که همینطور اتفاق افتاده اگر در این زمینه کم کاری گزارشهای تکان دهنده بیشتری در سالهای اینده دیده میشه و افراد بیشتری حالا چه شرکتها چه مشتریان چه شهروندان ضرر می کنن توی این زمینه و خسارتهای مادی و معنوی زیادی متحمل میشه بحث امنیت مسائل دیگرش انشاال... در فصل بیشتر دنبال خواهیم کرد.

توضیح بیشتر برای ارتش سایبری:

دولتها یک زیر ساختی رو دنبال می کنن که توی کشور ما اسمشو گذاشتن دولت الکترونیکی بعضی وقتا توی روزنامه ها و مجلات میبینیم که مثلا سازمان های دولتی میان هی امار میدن ، دولتها سعی میکنن یه پروژه ای رو دنبال کنن تحت عنوان خدمات الکترونیکی شهروندان ما یک مفهومی داریم تحت عنوان اقتصاد الکترونیک یعنی یک کاری بکنیم که یک درصد عظیمی از عملیات های اقتصادی کشور ها از طریق شبکه انجام بشه که بحث اصلیش بحث کم شدن ترافیک تو شهر ها هست ، کم شدن مصرف انرژی ، کم شدن آلودگی استفاده از خدمات الکترونیک به هزاران دلیل خیلی فواید زیادی برای اقتصاد داره پس بهتر انجام میشه پروژه هایی که دنبال میشه تحت عنوان اقتصاد الکترونیکی در کشور ما در قالب برنامه توسعه ۵ ساله ای که داریم دائم دولت وزارتخانه ها رو خود به خود شرکتهای دیگری هم که کار میکنن مجبور میشن که سالانه یه درصدی از فعالیتهاشون رو از حالت مکانیکی یا سنتی تبدیل کنن به خدمات الکترونیکی و باید این رو گزارش کنن به شورای عالی فنآوری

کشور که ما اینقدر بودجه کردیم و بودجه شم باید لحاظ بشه اما صرفا اینکارو کردن خیلی کار به موقع انجام نمیشه. در کنارش باید از این کار حفاظت بشه از این کار باید بشه به همین دلیل هست که دولت در قالب یک تشکیلات یک مجموعه ای رو تشکیل داده تحت عنوان ارتش سایبری که حالا زیر نظر سازمان های نظامی هم میتونه دنبال بشه یا وزارت دفاع . اینها کارشناسایی هستند که در بحث شبکه کنترل با traceing یا ردیابی های افراد در شبکه ها کار می کنن.

ارتش سایبری وظیفش این هست که دائم با این ساختارهای عظیم کشور رو رصد بکنه عملیات رو به صورت تصادفی سنجش بکنه مثلا ساختن نظام بانکی کشور رو کنترل بکنه شبکه سازمان تامین اجتماعی رو کنترل بکنه شبکه گمرکات بنادر رو کنترل بکنه . حالا حتما نمیخواد تک تک تراکنش های عملیات رو یکی یکی سند هاشو در بیاره و نگاه بکنه به صورت موردی .

مثلا مثال بزنیم در کشورمون یه مرز داریم دیدید مثلا یه جاهایی پایگاه مرزبانی وجود داره که روز یک عده ای میرن گشت میزنن این همین بعضی در فضاهای شبکه ها این افراد یوزرهایی دارن که یک سطح بالا بهشون دسترسی میده و توش رصد میکنن که الان مثلا آمار دادن . مثلال میزنیم در ساختار بانکی در استان کهکیلویه و بیر احمد روزانه مثلا ۶۰۰۰ میلیارد تومان تراکنش داره اگه یک دفعه مثلا دو برابر بشه یه جایی یه اتفاقی داره میفته یکی مثلا هک انجام داده حتی درصدها میتونه کم و زیاد بشه اما یک دفعه گزارش بشه میفهمن که دسترسی غیر مجاز داره اتفاق میفته حالا این وظیفه اون سازمان نیست که بخواد ردیابی کنه بازیابی کنه ارتش سایبری قضیه مراجع حقوقی و قانونی که هست این دنبال میشه فعلا ما این قضیه رو در سازمان های دولتی داریم . بخش اعظم اقتصاد ما اقتصاد دولتی هست بخش خصوصی هم قسمت اعظم کاراشون به سازمانها دولتی وابسته هست عملا اقتصاد خصوصیمون خیلی حجمش زیاد نیست ۲۰٪هست ۸۰٪ اقتصادمون دولتی ما داریم و دائم داریم بشه تعداد کاربرانشون زیاد میشه داره مثلا در دهه ۹۰ خورشیدی سالهای ۹۴-۹۰ نسبت به دهه ۸۰ دهه ۷۰ و دهه ۶۰ تعداد کاربران اینترنت توی کشور چقدر رشد کرده و بزرگ شده و این در سالهای آینده بیشتر خواهد شد. بنابراین این گستردگی باعث میشه خیلی خوب و باعث میشه اما یه جاهایی رشد بکنه اون ارتش

سایبری وظیفش اینه که زیر ساخت ملی رو کنترل بکنه مثلا فرض کنید مثلا ما از گمرک چهارمحال انتظار داریم روزانه ۲ میلیون تن کالا ورود داشته باشیم اینکه توش یکدفعه ۸ میلیون ثبت بشه میفهمن این آمارش عادی نبوده و دسترسی غیر مجاز داشته به همین دلیل از ارتش سایبری این وظیفه رو داره کنترل میکنه منتها شرکتها از این قضیه بی نسیب نیستند خیلی وقتها ترجیح میدن عملیاتشون رو زیر مجموعه دولتی دنبال بکنن و از خدمات و بخشنامه ها شون استفاده بکنن . امروزه در کشور ما مطمئن ترین شبکه ها شبکه های دولتی هستند و شبکه های دولتی چون یک تشکیلات عظیم پشتش هست و اینو کنترل میکنه اما شبکه های غیر دولتی ما اینگونه نیستند مثلا در ایران قسمت اعظم شهروندان ایمیلشون Gmailیا Yahoo هست که هیچ کدومش زیر مجموعه ارتش سایبری ایران نیست. به همین دلیل هست که شبکه های دولتی سیستم های شبکه ها انجام نمیدن زیر ساختهای خودشون رو میسازن احتمال دسترسی به برنامه ها و اسنادشون و مدارکشون هست قبول نمیکنن. مثال شما فرض کنید ما سال گذشته برای مجلمون توی ارشاد ، وزارت ارشاد برای تکمیل پرونده توی یه قسمتش باید آدرس ایمیل میذاشتیم این آدرس ایمیلهای اینجوری را قبول نمیکردن میگن حتما باید آدرس ایمیل دولتی باشه چون شرکتهای حقوقی نمیتونن به Yahooیا Gmailافراد عادی هم شما هیچ تضمینی ندارید شهروندان برای هم ایمیل میفرستن این هیچ مشکلی نداره ولی هیچ دلیلی نداره که اینا بخواد هک بشه یا مشکلی براشون بوجود بیاد اما در کشور ما خیلی از شرکتها و دولتها از این زیر سختهای استفاده نمیکنن.