به نام خالق یکتا

مقدمه

امروزه شبکه های سازمانی با تهدیدات بیشماری از جمله حملات هکرها، کدهای مخرب، حملات پیشرفته مداوم، حضور کارکنان کنجکاو و ناراضی و... روبرو هستند. از این رو یکی از بزرگترین نگرانی و چالش های پیش روی سازمان ها و بنگاه های کسب و کار چگونگی امن سازی یک شبکه مبتنی بر زیرساخت ها، نرم افزارها و سخت افزارهای فعلی آنها است. در حال حاضر مدیران شبکه رویکردهای مختلفی را برای امن سازی شبکه خود انتخاب می کنند مانند رویکردهای امنیت لایه ای. بدین منظور مدیر شبکه از ابزارهای مختلف برای امن سازی شبکه خود در لایه های مختلف رایانه کاربر، سرور، سوییچ ها و روترها و امنیت فیزیکی استفاده می کند. اما سوال مهمی که در اینجا مطرح است این است که آیا استفاده از این ابزارها برای امن سازی یک شبکه کافی است؟ آیا ابزارهای امنیتی می تواند به تنهایی با این تهدیدات پیچیده، پیشرفته و مختلف مقابله کند؟ آیا استفاده از ابزارهای امنیتی کفایت می کند یا باید از مولفه های دیگری در امن سازی استفاده نمود؟

در این خصوص تحقیقات مختلفی صورت گرفته است که در مجموعه ای از مقالات با عنوان "سازمان، امنیت اطلاعات و ..." به تشریح نیازمندی ها و مولفه های مرتبط با امنیت اطلاعات در سازمان ها، چگونگی طراحی و ایجاد امنیت در سازمان ها متناسب با ظرفیت و ساختار آنها خواهیم پرداخت.

نگاه اجمالی به رویکرد اشتباه مدیران سازمانی در امنیت اطلاعات

مدیران در جایگاه های مختلفی سازمانی که قرار دارند از مدیران عملیاتی گرفته تا مدیران ارشد سازمانی در خصوص بکارگیری فناوری اطلاعات و همچنین امن سازی آن مرتکب اشتباهات ناخواسته ای می گردند که موجب تضعیف امنیت اطلاعات، بوجود آمدن نقاط ضعف و آسیب پذیر در شبکه و سامانه های داخلی و حتی تهدیدات خارجی در فضای کسب وکار می شود.

از این رو شناخت این اشتباهات و توجه مدیران به اقدامات موثری که می توانند در جهت رفع این معایب بردارند بسیار ضروری است لذا به طور اجمالی اشتباهاتی را که مدیران در سازمان ها انجام می دهند بیان می گردد:

1. تحلیل و ارزیابی نادرست، غیرواقعی و نامتعارف تهدیدات و آسیب پذیری ها

برخی از مدیران سازمانی نمی توانند بدرستی وضعیت فعلی و آینده فضای فناوری اطلاعات سازمان خود را ترسیم نموده و ریسک ها و تهدیدات متصور برای این فضا را تحلیل نمایند. غالبا تهدیدات را جدی نگرفته یا آنها را بزرگنمایی می کنند به عنوان مثال تفکر نادرست مدیران به صورت زیر است:

- این تهدید برای سازمان ما متصور نیست.

- سازمان ما اطلاعات با ارزشی دارد که با سیستم های فعلی امن نمی شود و باید هزینه بالاتری به آن اختصاص داد.
- همه تهدیدات داخلی و خارجی در مورد اطلاعات سازمان ما وجود دارد.

این در حالی است که وجود یک تحلیل درست از این وضعیت می تواند منجر به امن سازی صحیح، انتخاب درست تجهیزات و خدمات، صرف منابع مالی و نیروی انسانی مناسب و ... گردد.

2. استفاده نکردن از کارشناسان مجرب در حوزه امنیت اطلاعات و نگاه ابزار محوری

در حوزه امنیت فناوری اطلاعات دانستن این نکته ضروری است که "ابزارها در کنار انسان، باهوش، کارا و اثربخش می شوند". این بدان معنی است که تکیه بر ابزارهای سخت افزاری و نرم افزاری بدون استفاده از نیروی انسانی مجرب و آگاه علاوه بر اینکه امنیت کافی را بوجود نمی آورد بلکه باعث آسیب ها و حفره های امنیتی ناشی از عدم دانش و آگاهی می شود. این عامل انسانی است که می تواند خروجی تجهیزات امنیتی را تجزیه و تحلیل و تفسیر نماید زیرا ابزارها دارای مثبت کاذب (false positive) هستند که ممکن است حتی بسیاری از عملیات درست و مجاز را نیز قطع و مانع از دسترسی ها شود.

کارشناسان مجرب با دانستن بسیاری از اصول، کاربردها، تکنیک ها، بهینه روش ها (best practice) و استانداردها و نحوه بکارگیری آنها می توانند امنیت پایدار و قابل اعتمادی را فراهم نمایند که کاربران در آن محیط علاوه بر حس امنیت، می توانند از امکانات به نحو ساده تر و مطلوبتری استفاده نمایند.

برخی اوقات مدیران نسبت به انتخاب افراد خبره و اهل فن دچار مشکل شده و افراد شایسته و دارای توانمندی های این مشاغل را انتخاب نمی کنند و از کارشناسان شبکه، نرم افزار نویسان و ... بدون بهره مندی از تجارب امنیتی در جایگاه های حرفه ای امنیت استفاده می کنند.

3. مشاوره نگرفتن از متخصصین و شرکت های با تجربه در این حوزه

امنیت اطلاعات مجموعه ای از دانش، تجربه، ابزار، هوش، هزینه، ارتباطات، همکاری های واقعی و مجازی افراد، شرکت ها و انجمن ها و... در کنار هم است. در اصل امنیت اطلاعات و مولفه های آن یک مقوله ثابت و محدود نیست بلکه یک پدیده پویا و در جریان است که پیشرفت و موفقیت در آن نیازمند تعامل و ارتباط بین بازیگران این حوزه است. یک سازمان برای اینکه بتواند در این حوزه موفق باشد باید بتواند با بازیگران موثر این حوزه از جمله شرکت های موفق در زمینه امنیت اطلاعات ارتباط پویا و سازنده ای را برقرار نماید و از دانش و تجربه آنها استفاده نماید. اتکا به نیروهای داخلی و بخش های خارجی غیرمتخصص و ناتوان می تواند موجب گمراهی سازمان ها، تصمیم گیری های غیرمنطقی و نامناسب، استفاده از فناوری های غیرضروری و تحمیل هزینه های نامتعارف به سازمان ها گردد.

4. کندی و ناتوانی در تصمیم گیری ها در خصوص تامین و استفاده از تجهیزات، محصولات و خدمات امنیتی

یکی از مهمترین اصول در برقراری و حفظ امنیت اطلاعات، تصمیم گیری به موقع در استفاده از تجهیزات و خدمات امنیتی متناسب با تهدیدات روز و مرتبط با سازمان است. گاه اتفاق می افتد که یک سازمان با تهدیدی ساده و معمولی روبرو است و کارشناسان این حوزه تهدید را شناسایی نموده و برای مقابله با آن راه حل های امنیتی را ارائه می دهند. اما در هنگام تصمیم گیری در خصوص رفع این تهدید، مدیران سازمانی نمی توانند تصمیم مناسبی را در خصوص تامین منابع مورد نیاز مالی، نیروی انسانی و ... گرفته و محصول یا خدمت مورد نظر به موقع در اختیار کارشناسان قرار نمی گیرد. این امر موجب می شود امنیت اطلاعات سازمان با تهدیدی بسیار جدی مواجه شود. از چالش های موجود در تصمیم گیری مدیران می توان به موارد زیر اشاره نمود:

- نبود یا عدم اعتماد به عوامل تصمیم ساز مانند نداشتن معیارها و شاخص های انتخاب، نداشتن سازوکار برای مقایسه محصولات و خدمات، فقدان یا عدم اعتماد به کارشناسان خبره
- نداشتن شناخت و درک درستی از وضعیت امنیت اطلاعات و تهدیدات آن
- نداشتن ثبات و پایداری لازم در انتخاب یک محصول مناسب با توجه به نیاز سازمان

5. برون سپاری پروژه های امنیت اطلاعات به شرکت ها و افراد غیرمتخصص

برون سپاری در سازمان ها که با اهداف کاهش هزینه ها، صرف نیروی سازمان در جهت اهداف اصلی و مهمتر، ارتقا کیفیت و تمرکز بر شایستگی های محوری سازمان صورت می گیرد در حوزه امنیت اطلاعات نیز بسیار کاربردی و رایج است. اما باید در نظر داشت که کدامیک از پروژه های امنیت اطلاعات در سازمان باید برون سپاری شده و به کدام بخش برون سپاری گردد.

پروژه های امنیت اطلاعات در سازمان ها بسیار متنوع است از این رو غالبا نیروی انسانی لازم برای تامین و تهیه آنها در اختیار سازمان ها نیست لذا باید در نظر داشت پروژه هایی که دارای ویژگی های زیر است ترجیحا برون سپاری گردد:

- تولید آن برای سازمان هزینه بسیار بالایی دارد. در مورد خدمات باید گفت که هزینه بالا در آموزش نیروی انسانی، یادگیری فرآیندها، تامین سامانه های نرم افزاری و سخت افزاری مرتبط با خدمت و... است.
- سازمان قادر نیست با نیروهای فعلی آن را تهیه کند.
- برون سپاری آن به اهداف و ماموریت کسب و کار سازمان آسیب وارد نمی کند.
- مزیت رقابتی و شایستگی محوری آن سازمان نیست.

از این رو باید افراد، بخش ها و شرکت هایی را برای این منظور انتخاب نمود که با رعایت عدم افشای اطلاعات، تخصص کافی در پذیرش و انجام این گونه پروژه ها را داشته باشد. به عنوان مثال انتخاب شرکتی که تاکنون پروژه ای در زمینه تست نفوذ را انجام نداده است، برای انجام این خدمت امری اشتباه است زیرا موجب می شود شناخت درستی از آسیب پذیری ها و تهدیدات شرکت صورت نگرفته و نقاط ضعف آنها شناسایی نشود. همچنین تامین ضدبدافزاری که به لحاظ

نصب و به روز رسانی مدیریت یکپارچه ندارد و متناسب با نیاز سازمان نیست، می تواند باعث گسترش بدافزار در سازمان و تخریب اطلاعات شود.

6. استفاده نادرست از سامانه ها در امن سازی فضای فناوری اطلاعات

در امنیت اطلاعات محصولات متنوعی توسط شرکت های امنیتی تهیه شده و به بازار امنیت اطلاعات عرضه شده است که می تواند در لایه های مختلف دفاعی و با اهداف متفاوت ممانعتی (مانند ضدبدافزار،UTM، DLP، SIEM) ، شناسایی کننده (IDS و مانیتورینگ) و پشتیبانی کننده به کار گرفته شود. اما در بسیاری از مواقع مدیران در انتخاب و بکارگیری این تجهیزات و سامانه ها دچار اشتباهاتی می شوند از جمله

- تفکر و بینش غلط "وجود امنیت کامل و صددرصدی" از اطلاعات، سامانه ها، شبکه ها و تجهیزات
- تکیه زیاد به دفاع در لایه شبکه
- اهمیت ندادن به امنیت نرم افزارها
- اعتماد بیش از اندازه به ابزارها و فناوری
- استفاده نکردن از محصولات امنیتی به صورت یکپارچه و همگرا در سطوح مختلف پیش بینی و جلوگیری از حملات، شناسایی تهدیدات و حملات، پاسخ و مقابله با تهدید، مانیتورینگ و نظارت بر امنیت

7. بکارنگرفتن خدمات امنیتی مرتبط با شبکه ها و سامانه های اطلاعاتی سازمان

همانگونه که بخشی از امنیت اطلاعات استفاده از تجهیزات و سامانه های امنیتی است بخش دیگر آن تکیه بر خدمات امنیتی از جمله طراحی و اجرا، مشاوره و آموزش، کنترل امنیت و واکنش در برابر حوادث امنیتی است. این خدمات در کنار محصولات قرار می گیرد تا امنیت پایدارتری را بوجود آورد. گاها مدیران سازمانی به استفاده از یک ابزار امنیتی بسنده کرده و از تامین خدمات امنیتی خودداری می کنند در صورتی که طراحی امنیتی فضای تبادل، نگهداری و پردازش اطلاعات سازمان مهم و ضروری است. همچنین آموزش کارکنان از جمله مواردی مهمی است که در باید در امنیت در نظر گرفته شود زیرا نیروی انسانی آسیب پذیرترین قسمت امنیت اطلاعات یک سازمان است.

8. نبود طرح ریزی و اعمال فرآیند ها و سیاست های امنیتی مناسب

بخش عمده ای از امنیت علاوه بر محصولات و خدمات، انتخاب فرآیندها و قواعد امنیتی است که یک سازمان باید با توجه به محیط و فرهنگ سازمانی خود و اهمیت اطلاعاتش آنها را طرح ریزی و اجرا نماید. انتخاب فرآیند ها و سیاست امنیتی مناسب می تواند جلوی بسیاری از رخنه های امنیتی را گرفته و سطح امنیت اطلاعات سازمان را ارتقا بخشد. در برخی سازمان ها چالش جدی در این زمینه وجود دارد که در زیر به برخی از آنها اشاره می شود:

- طرح امنیتی و دفاعی و بازیابی خرابی در مواقع بحران وجود ندارد.
- اولویت بندی در امنیت دارایی ها و تجهیزات و اطلاعات سازمانی صورت نگرفته است.

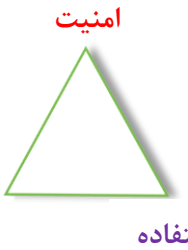
- از فرآیندهای یکپارچه و مجتمع در امن سازی استفاده نشده است .

9. حمایت نامناسب مدیران ارشد سازمانی از بکارگیری محصولات و خدمات امنیتی

به منظور رسیدن به سطح امنیتی مورد انتظار، مدیران ارشد باید از پیاده سازی و بکارگیری سامانه ها و اجرای خدمات امنیتی در سازمان حمایت کنند چرا که در نظر کارکنان، امنیت با سادگی و راحتی در تضاد است و موجب می شود مقاومت هایی در نصب و راه اندازی سامانه های امنیتی صورت گیرد. از این رو مدیران ارشد با حمایت خود می توانند جلوی کارشکنی ها، جبهه گیری و مقاومت ها را گرفته و بهره برداری از سامانه را تسریع بخشند.

10.عدم توجه به چالش افزایش امنیت و امکان کاهش کارایی و سادگی در استفاده از فناوری اطلاعات

از مشکلترین و سخت ترین موضوعاتی که در ایجاد امنیت اطلاعات وجود دارد موازنه و تعادل بین سه ضلع مثلث امنیت اطلاعات، سادگی در استفاده و عملکرد است. امنیت اطلاعات موانعی را برای جلوگیری از حملات بوجود می آورد که موجب می شود عملکرد و سادگی در استفاده برای کاربران کاهش یابد.



این مساله مهمی است که مدیران از آن غافل می شوند و بعضی اوقات استفاده از ابزارهای امنیتی یا یک سیاست امنیتی را در سازمان الزامی دانسته ولی سازوکار لازم برای آن را درنظر نمی گیرند. به عنوان مثال امروزه مساله BYOD (استفاده از ابزارهای شخصی مثل تبلت و گوشی در محل کار است) و پردازش و ذخیره سازی ابری در سازمان ها به عنوان یک چالش امنیتی محسوب می شود که مدیران برای رفع این نگرانی، سیاست امنیتی را اجرایی می کنند که ممکن است موجب نارضایتی و کاهش عملکرد کارکنان گردد. مدیران موظفند برای مقابله با اینگونه چالش ها تدابیر لازم مانند اطلاع رسانی، فرهنگ سازی و ... اتخاذ نمایند. به هر حال نگرش و راهبرد موازنه امنیت، سادگی در استفاده و عملکرد مساله ای است که مدیران نباید از آن غفلت کنند.

11.عدم توجه به مساله هزینه- فایده در تهیه و بکارگیری خدمات و محصولات امنیتی

آنچه در حوزه فناوری اطلاعات و کاربردهای آن مطرح این است که بهره برداری از آن هزینه بر است. این قاعده در زمینه امنیت اطلاعات نیز صادق است و نباید فراموش کرد که"*امنیت هزینه دارد و برای طراحی، ایجاد، کنترل و بهبود آن باید هزینه کرد.*" این هزینه ها ناشی از تهیه محصولات امنیتی یا خدماتی می شود که برای سازمان ارزشمند است در واقع این هزینه ها باید منجر به بکارگیری محصولی یا خدمتی شود که اقدامات امنیتی ممانعتی، پیشگیرانه، شناسایی کننده و مقابله کننده را برای سازمان به همراه داشته باشد. تخصیص ندادن هزینه های منطقی و مناسب برای تجهیزات یا خدمات ممکن است تهدیدات متصوره برای دارایی های سازمان را از بین نبرده و حتی باعث آسیب پذیری های جدی تر و جدیدتری نیز گردد.

همچنین پرداخت هزینه های گزاف و بیش از حد برای بکارگیری یک سامانه ممکن است باعث اتلاف منابع مالی سازمان گردد. از این رو شناخت دارایی ها و ریسک های متصور برای آن و سپس اقدام متقابل برای رفع آن با هزینه متناسب باید به عنوان یک اصل کلی در امنیت لحاظ شود. لذا باید سنجید که دارایی و اطلاعات چه مقدار با ارزش است و سازمان برای آن حاضر است چه مقدار هزینه کند همچنین عواملی مانند اعتبار سازمان نیز باید درنظر گرفته شود. به عنوان مثال مراکز نظامی، زیرساخت های حیاتی کشورها و بانک ها از جمله مراکزی هستند که صرف بودجه و هزینه در حوزه امنیت بهره و ارزش زیادی دارد.

مدیران گاها نگرش درستی در این خصوص ندارند و ممکن است تجهیزاتی را تهیه کنند که بسیار گران بوده و هزینه بالایی دارند اما از نظر کارکرد یا سهم دارایی، ارزش آن هزینه را ندارد و در نتیجه سازمان با صرف این هزینه نه تنها فایده و بهره بیشتری کسب نکرده بلکه منابع مالی خود را نیز به هدر داده است. در نقطه مقابل ممکن است مدیران آن چنان برای امنیت هزینه نکرده و ریسک های امنیتی را افزایش دهند.

12.نبود اطلاع رسانی درست و به موقع و توجیه مدیران و کارکنان و نقش آنها در امن سازی

یکی از بزرگترین تهدیدات در حوزه امنیت اطلاعات ناشی از تهدیدات داخل سازمانی و کارمندان ناراضی یا کنجکاو است. اعتماد بیش از حد و نامتعارف به کارکنان داخلی یا عوامل خارجی مانند شرکا و همکاران سازمانی، عدم استفاده از آموزش های تخصصی و عمومی (مانند رها نکردن رایانه ها بدون ملاحظات امنیتی، بازنکردن ایمیل های ناشناس و انتخاب کلمه عبور نامناسب و ضعیف، گم شدن یا سرقت تجهیزات حاوی اطلاعات) خطرات جدی را برای یک سازمان به همراه دارد. مدیران سازمانی باید بتوانند علاوه بر کسب مهارت ها و دانش لازم در این خصوص، اقداماتی را برای آموزش کارکنان انجام دهند و همچنین با توجیه درست و به موقع بالادستی ها بتوانند منابع مالی، تجهیزاتی و نیروی انسانی مورد نیاز در حوزه امنیت را تامین نمایند. به عنوان مثال تفکر و نگرش کارکنان در بکارگیری محصولات امنیتی مساوی با کندی سیستم، نبود حریم خصوصی و سخت شدن رویه های کاری است که مدیران با توجیه، اطلاع رسانی و آموزش و استفاده از محرک انگیزشی کارکنان می توانند ذهنیت و فرهنگ جاری را به نحو مطلوبی تغییر دهند.

13.استفاده نکردن از استانداردها، بهینه روش ها و راهنمای امن سازی فضای فناوری اطلاعات سازمان

استاندارد های امنیتی به ایجاد امنیتی مورد انتظار در سازمان ها کمک می کنند ولی برخی مدیران از روش ها و رویه های غیر استاندارد، غیراصولی و سلیقه ای برای امنیت استفاده می کنند که موجب کاهش امنیت نیز می گردد. به عنوان نمونه استفاده از UTM به منظور امن سازی لایه شبکه و سرورها، استفاده از رمزنگاری برای امنیت داده ها و استفاده از WAF برای امنیت سرورها و برنامه های کاربردی آن در یک شبکه مبتنی بر استانداردهای امنیتی پیشنهاد می گردد اما مدیران ممکن است فقط به استفاده از رمزنگاری به عنوان اصلی ترین روش امن سازی اکتفا کنند که بینشی غلط است. استانداردها و بهینه روش ها ناشی از دانش، تجربه، سعی و خطا، آزمودن ها و صرف هزینه های گزاف و همکاری بسیاری از افراد، شرکت ها، موسسات و حتی کشورها است که به یک استاندارد و روش بهینه منتج شده

است و بهره نگرفتن مدیران از آنها باعث حرکت رو به عقب و از دست دادن اطلاعات و تحمیل هزینه های هنگفت به سازمان می شود.

نتیجه

در این مقاله سعی شد که اشتباهات رایج مدیران در حوزه امنیت اطلاعات تشریح و بررسی گردد و ممکن است چالش ها و مسائل دیگری نیز باشد که در این مقاله بیان نشده است. توجه به موارد بالا می تواند به مدیران سازمان ها کمک کند تا در دام این اشتباهات نیافتند و امنیت اطلاعات سازمان خود را به مخاطره نیاندازند. نگرش اشتباه، تحلیل نادرست، وابستگی به ابزار و استفاده نکردن از نیروی انسانی مجرب، عدم مشاوره، تصمیم گیری کند و نادرست، نبود حمایت مدیران ارشد، تامین نامناسب محصولات و خدمات امنیتی و واگرا، صرف هزینه نامتناسب، عدم توجه به استانداردها، آموزش، عملکرد و کارایی از جمله چالش هایی است که مدیران گاها با آن روبرو می شوند و باید برای حفظ امنیت اطلاعات سازمان نسبت به کاهش و رفع آنها اقدام نمایند.