به نام خالق یکتا

اصول امنیت اطلاعات (اصول مقدماتی و پیش نیاز)

مقدمه

با توجه به اهمیت نقش و جایگاه امنیت اطلاعات برای مقابله با تهدیدات مختلف و پیشرفته، سازمان ها به خصوص مدیران ارشد و تصمیم گیرندگان آن با چالش های جدی در خصوص امنیت اطلاعات روبرو هستند. یکی از این چالش ها و سردرگمی ها انتخاب راه حل های امنیتی برای سازمان خودشان است. برای خروج از این سردرگمی ها، سازمان ها ابتدا باید اجزا مورد تهدید، نیازها و اصول امنیتی را بشناسند و به این سوالات کلیدی پاسخ دهند که "چه اجزایی از سازمان باید امن شوند؟" و "اصول و پایه های امنیت اطلاعات در یک سازمان چیست؟".

به عنوان مثال سازمانی از یک پورتال اداری برای ارتباط و انجام ماموریت بخش های خود که به طور جغرافیایی در یک کشور پراکنده هستند، استفاده می کند. مدیران سازمانی با این مشکل روبرو هستند که چه اجزایی از سامانه های اجرایی و اطلاعاتی، تجهیزات ارتباطی و زیرساخت های خود را امن نمایند. یا به عبارت دیگر آیا فقط امنیت زیرساخت کافی است؟ آیا توجه به امنیت نیروی انسانی نیاز است؟ آیا نیاز سازمان در استفاده از تجهیزات امنیتی است؟ و سوال های دیگری که ممکن است مدیران با آن روبرو شوند.

برای پاسخ به این سوال ها لازم است در ابتدا یک سازمان اصول و پایه های امنیتی را که برای مقابله با تهدیدات لازم است بشناسد و سپس در خصوص استفاده و بکارگیری آنها اقدام نماید. بدین منظور در این مقاله به تشریح اصول و پایه های کلی امنیتی می پردازیم:

اصول و قواعد امنیت اطلاعات

1- **مدیریت ریسک:** مدیریت ریسک فرآیندی است که در آن ریسک شناسایی، تحلیل و ارزیابی شده و گام های کاهش ریسک تا رسیدن به سطح قابل قبول برداشته می شود. مدیریت ریسک باید مبتنی بر درک جامعی از وضعیت امنیت اطلاعات سازمان باشد به عبارت دیگر امنیت اطلاعات با روش های مدیریت ریسک فراگیر ترکیب شود. رویکرد مدیریت ریسک باید به عنوان فرآیندی برای تعادل بین اقدامات و هزینه های اقتصادی برای محافظت از اطلاعات و سامانه ها پیاده سازی و بکار گرفته شود.

فرآیند شناخت، تحلیل و ارزیابی ریسک های امنیت اطلاعات می تواند به سازمان ها برای انتخاب کنترل های امنیتی مناسب با محیط کسب وکارشان کمک شایانی نماید.

2- **نقش ها و مسئولیت ها:** نقش ها و مسئولیت ها باید براساس جایگاه سازمانی به کارکنان سازمان اعطا گردد و متناسب با وظایف آنها، سطوح اختیارات افراد و دسترسی به اطلاعات و منابع تعریف گردد. سازمان نیاز به یک چارچوب حاکمیت امنیت اطلاعات موثر دارد تا به تصمیم گیرندگان سازمان در فهم جامع و دقیق از محیط تهدید کمک کرده در نهایت بتوانند تصمیمات مبتنی بر ریسک مناسبی را اتخاذ کنند. همچنین این چارچوب به جوابگویی مناسب همه وظایف کمک می کند. در واقع وظایف و نقش ها باید به طور کامل شفاف، همراه با افزایش راستی و درستی در انجام کارها بر اثر کاهش تضاد در وظایف و تفکیک مناسب وظایف باشند.

3- **مستندسازی امنیت اطلاعات:** مستندسازی برای هر روش و مکانیزم امنیت اطلاعات حیاتی است و باید رویه ها و سیاست ها در آن مستند سازی گردد. آنچه باید مستند سازی شود شامل سیاست های امنیتی، طرح مدیریت ریسک امنیتی، طرح امنیتی سامانه ها و شبکه، رویه های عملیاتی استاندارد، طرح پاسخ به رخداد، رویه های اضطراری و طرح بازیابی خرابی و تداوم کسب و کار است.

طبق آمار منتشره توسط شرکت سیسکو، 75٪ شرکت ها در 10 کشور پیشرفته دارای سیاست های امنیتی در شبکه شان هستند و این درحالی است که 40٪ از کارکنان و 20٪ از متخصصین فناوری اطلاعات آنها نمی دانند که سیاست های امنیتی وجود دارد.

4- **اعتباربخشی سامانه ها:** سازمان باید از وجود سطح امنیتی مناسب برای اطلاعات و سامانه های خود اطلاع پیدا کند و بفهمد تا چه سطحی از ریسک باقی مانده قابل قبول است. برای این منظور نیاز است تا ممیزی امنیتی برای تمامی اطلاعات طبقه بندی شده و سامانه ها و شبکه ها براساس استانداردها صورت گیرد. این عملیات توسط ارزیاب های رسمی امنیت اطلاعات انجام می شود. پس از ارزیابی گواهی نامه رسمی دریافت می گردد. با توجه به شناخت میزان ریسک، باید راه حل های امنیتی به منظور ارتقا امنیت تامین و بهره برداری شود.

5- **مانیتورینگ امنیت اطلاعات:** امنیت اطلاعات یک فرآیند مداوم است و اطمینان از امنیت باید در همه زمان ها باشد. آسیب پذیری ها می تواند با یک طراحی و پیاده سازی ضعیف، مدیریت تغییرات یا نگهداری و همچنین تغییر در فناوری ها یا روش ها و مکانیزم های حمله بوجود آید. روش های مانیتورینگ به شناخت آسیب پذیری های جدید و نگهداری امنیت در برابر حوادث و تغییرات ناشناخته کمک می کند. در عملیات مانیتورینگ علاوه بر نظارت بر کارایی و عملکرد سامانه ها و منابع مختلف می توان به مدیریت آسیب پذیری ها (کشف، ارزیابی، تحلیل و مقابله با آنها) و مدیریت تغییرات (اعمال تغییر در سامانه ها، شناسایی اختلالات و نواقص و رخنه ها، تحلیل و رفع نابسامانی و آسیب در هنگام تغییر) نیز پرداخت.

6- **رخدادهای امنیت سایبر:** رخدادهای امنیتی در فضای سایبر می تواند تاثیر بسزایی در تخریب عملیات کسب و کار یک بنگاه داشته و باعث تحمیل هزینه ها، افشا اطلاعات مشتریان و خدشه دار شدن اعتبار بنگاه یا حتی دولت ها شود. بدین منظور نیاز است اقدامات موثری برای مقابله با رخدادهای امنیتی انجام شود. استفاده از رویه ها و ابزارهای شناسایی و کشف رخدادها، به روز نگه داشتن سامانه ها در محیط تهدید، گزارش دهی مناسب رخدادها و مدیریت رخدادها با ضبط رخداد، تخصیص مسئولیت، مدیریت داده ها در برابر اثر کدهای مخرب و حفظ صحت آنها از اقدامات موثر است.

براساس آمار موسسه وریزون در سال 2014 بیشترین صنایعی که مورد تهاجم کدهای مخرب قرار گرفته اند، بخش های دولتی، فناوری اطلاعات، خدمات شهری و تولیدی بوده اند.

7- **تعامل با صنعت و برون سپاری:** برون سپاری می تواند در انتخاب گزینه های مختلف برای تامین خدمات فناوری اطلاعات با هزینه مناسب و خدمات بهتر کمک نماید. البته ممکن است با ریسک هایی از جمله قرار گرفتن اطلاعات در مکان های نامناسب و دسترسی افراد بیشتر به اطلاعات همراه باشد که منجر به افشا و نشت اطلاعات گردد.

محاسبات ابری یکی ازمهمترین تغییرات را در دهه آینده در تکنولوژی ارتباطات و اطلاعات بوجود خواهد آورد به این صورت که با ایجاد زیر ساخت هایی با مزایای مالی و عملیاتی روشن برای سازمان ها، آنها ترغیب به استفاده از آن می گردند. این در حالی است که اتصال به اینترنت ذات این فناوری بوده و اطلاعات باید در اینگونه شبکه ها و سرورها ذخیره شوند. با این حال فعالیت های مخرب سایبری علیه این فناوری در حال گسترش است و یکی از تهدیدات عمده سازمان ها می تواند در دهه آینده استفاده از این فناوری بدون در نظر گرفتن ملاحظات امنیتی و روش های امن باشد.

شرکت های متعددی اقدام به تامین و توسعه زیرساخت های این فناوری برای سازمان و بنگاه های دیگر نموده اند که حفظ امنیت اطلاعات و جلوگیری از افشا آن یکی از چالش های آینده محسوب می گردد.

توجه به این نکته ضروری است که انتخاب شرکتی برای برون سپاری و ارتباط با صنایع مختلف باید براساس اطمینان از حفظ محرمانگی، صحت و دسترس پذیری اطلاعات باشد.

براساس آمار منتشره سال 2012 از سوی موسسه پونمون 41٪ از نشت اطلاعات سازمان از سوی شرکت هایی بوده که پروژه به آنها برون سپاری شده یا همکار تجاری و یا تامین کنندگان ابر (Cloud) بودند که به اطلاعات سازمانی دسترسی داشتند.

نتیجه

در این مقاله 7 اصل از اصول امنیت اطلاعات ارائه شد که می تواند به عنوان اصول مقدماتی و اولیه امنیتی درنظر گرفته شود. به منظور رعایت این اصول نیازی به استفاده از ابزارهای تخصصی و پیشرفته نبوده و سازمان ها می توانند با صرف حداقل

هزینه ها به این اصول دست یابند و با مدنظر قراردادن آنها پایه های امنیتی خود را شکل داده و به بینش مناسبی برای طراحی امنیتی و پیاده سازی آنها برسند.

در مقاله بعدی به ارائه سایر اصول امنیتی از جمله امنیت فیزیکی، نرم افزار، ارتباطات و کارکنان، مقوله رمزنگاری و کنترل دسترسی و امنیت دامنه ها و شبکه پرداخته می شود.

مراجع

Department of Defence-Intelligence and Security group. (2014). *Australian Government Information Security Manual-PRINCIPLES.* Australian Government.