به نام خالق یکتا

اصول امنیت اطلاعات (اصول و قواعد پایه)

در ادامه مبحث ارائه شده در خصوص اصول امنیت اطلاعات در مقاله قبل که به معرفی اصول مقدماتی و پیش نیاز پرداخته شد، در این مقاله به معرفی و بررسی سایر اصول و قواعد امنیت اطلاعات که به عنوان قواعد اصلی و پایه ای در نظر گرفته می شوند، می پردازیم:

8- **امنیت فیزیکی**: امنیت فیزیکی یکی از اقدامات پایه ای در امنیت اطلاعات محسوب می شود. بدون کنترل های کافی در امنیت فیزیکی، سایر تلاش ها برای امن سازی اطلاعات بسیار سخت و حتی غیرممکن است. امنیت فیزیکی نیاز به زیرساخت ها و تجهیزاتی دارد که بتواند خطر سرقت، تخریب و دستکاری را کاهش دهد. امنیت فیزیکی به صورت تک لایه ای مانند کنترل تردد به ساختمان برای مقابله با خطرات کافی نیست و نیاز است از یک رویکرد لایه ای برای کاهش دسترسی های غیرمجاز و خرابی سامانه ها و تجهیزات استفاده شود. در این راستا باید از تجهیزات مختلف و چیدمان لایه ای برای دسترسی مجاز به سامانه ها، زیرساخت شبکه، تجهیزات فناوری اطلاعات و ارتباطات و رسانه ها استفاده کرد. از جمله تجهیزات می توان به کنترل تردد و احراز هویت چندعاملی، دوربین های نظارتی، اطفاء حریق و... اشاره نمود.

9- **امنیت کارکنان**: کارکنان به عنوان افرادی که می توانند به طور مجاز و قانونی به امکانات، دارایی ها، سامانه ها و سایر افراد سازمان دسترسی داشته باشند، ممکن است به طور عمدی یا غیرعمدی اقدام به بهره برداری غیرقانونی و آسیب رساندن به آنها نماید. سازمان ها باید با شناخت تهدیدات داخلی و استفاده از یک چارچوب مشخص برای امنیت کارکنان، ریسک های ممکن را مدیریت نمایند. حضور کارکنان در اقدامات خرابکارانه، افشای اطلاعات و سرقت تجهیزات، می تواند نقش مهمی را در تخریب اعتبار، عملیات، بهره وری و مالی سازمان داشته باشد. ناآگاهی کارکنان در مورد مسئولیت های امنیتی شان و نقش آنها در حفاظت از سامانه ها و اطلاعات، موجب خرابکاری های غیرعمدی می شود. به عنوان مثال تلاش های مهندسی اجتماعی با هدف سو استفاده از کارکنان در دسترسی ها و دانسته های آنها، می تواند اثرات زیانباری را به همراه داشته باشد و اطلاعات حساسی افشا گردد. بنابراین ایجاد فرهنگ اطلاع رسانی امنیت از طریق جلسات و برنامه های آموزشی مداوم به منظور ارتقا سطح آگاهی تمامی کارکنان از نقش ها، وظایف و مسئولیت هایشان، انواع حملات و روش های مقابله یک مقوله حیاتی است. همچنین سازمان باید در خصوص آشنایی کارکنان در استفاده از اینترنت اطمینان حاصل کند و تمامی ملاحضات و نکات امنیتی را در هنگام استفاده از اینترنت به آنها متذکر شود. به عنوان مثال در یک سازمان هنگامی که کارکنان از طریق یک ایمیل یا نرم افزار P2P فایلی را دریافت می کنند ممکن است با دور زدن سیاست های امنیتی، نا خواسته کدمخرب و ویروسی را وارد سازمان نمایند که برای مقابله با این گونه خطرات باید کارکنان آموزش لازم را در خصوص ویروس یابی فایل ها قبل از استفاده از آن و انتقال به شبکه، دریافت نمایند. همچنین استفاده از نرم افزارهای P2P که از VOIP استفاده می کنند مانند skype یا سایر نرم افزارهایی که می تواند با پروتکل های خاص فایروال را دور بزنند، موجب ایجاد نقاط دسترسی آسیب پذیر در سامانه ها می شود.

با آگاهی دادن به کارکنان در خصوص نرم افزارهای غیرمجاز و مخرب و پروتکل های مختلف و خدمات اینترنتی، سازمان ها می توانند جلوی بسیاری از تهدیدات را بگیرند.

10- **زیرساخت ارتباطات**: با گسترش زیرساخت های ارتباطی سامانه ها و شبکه ها، مدیریت کابل قوی می تواند به حفظ صحت و دسترسی پذیری ارتباطات و محرمانگی و صحت اطلاعات کمک شایانی نماید. مدیریت کابل مناسب، احتمال دسترسی غیرمجاز به طور سهوی یا عمدی را کاهش می دهد. قرار دادن کابل ها به صورت کنترل شده و اطمینان از برچسب گذاری و جداسازی مناسب و امکان دسترسی آسان به آنها جهت بازدید ها می تواند به شناسایی دستکاری های پنهانی یا دسترسی غیرمجاز به کابل ها و اطلاعات توسط عامل مخرب یا خرابی زیرساخت ارتباطات که تاثیر زیادی بر دسترس پذیری اطلاعات دارد، کمک کند. برچسب گذاری کابل ها همچنین می تواند از اتصال تصادفی یک سامانه به سامانه ای دیگر با طبقه بندی پایینتر را که باعث نشت اطلاعات می شود، جلوگیری نماید.

سرمایه گذاری در زمینه مدیریت کابل و ایجاد زیرساخت های مناسب مانند استفاده از فیبرنوری علاوه بر کاهش تهدیدات پیش بینی نشده، سرعت بالاتری را در انتقال اطلاعات فراهم می کند. پیاده سازی در دسترس و قابل مشاهده زیرساخت های کابل باعث کاهش اقدامات هزینه بر در آینده مانند به روز رسانی، اعتبار بخشی و ممیزی، یافتن خطا، مدیریت تنظمیات و بازرسی های نوبه ای برای کشف دستکاری و خرابکاری می شود.

خطر تشعشع از تجهیزات و کابل ها فرصتی را برای شنود و رهگیری اطلاعات حساس و طبقه بندی شده فراهم می کند. بعضی از محیط ها که گسترده و در مکان های بیشتری فراگیر شده اند، امکان حملات مبتنی بر تشعشع و پرتوهای سیگنالی را افزایش می دهد. بدین منظور با استفاده از زیرساخت های مناسب کابل و روش های نصب و راه اندازی مطمئن و ایمن در برابر خطر پرتوها مانند شیلد کردن، می توان امنیت اطلاعات را افزایش داد.

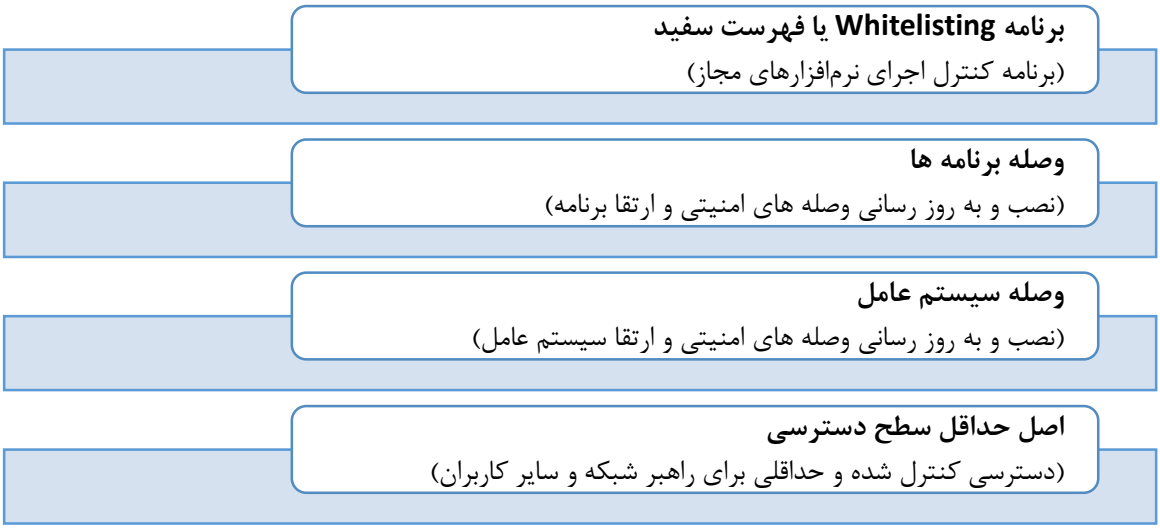
11- **ابزارها و سامانه های ارتباطی**: این ابزارها نقش دروازه دیجیتالی برای ورود و خروج اطلاعات به یک شبکه را ایفا می کند و باعث تسهیل افشای اطلاعات به صورت عمدی یا سهوی می شود. به عبارت دیگر این ابزارها یک نقطه دسترسی به سامانه ای را که به آن متصل هستند، به شمار می آیند.

تدوین و بکارگیری سیاست ها و رویه های استفاده از این ابزارها نقش ویژه ای را در کاهش احتمال نشت اطلاعات را بازی می کند به گونه ای که کارکنان اطلاع کافی را از خطرات و روش های حفاظت از اطلاعات در هنگام اسکن، کپی، چاپ و انتقال را کسب نمایند. همچنین موقعیت فیزیکی و نحوه قرارگیری این ابزارها نیز در دسترسی غیرمجاز به آنها تاثیر دارد.

این ابزارها شامل ابزارهای رادیویی و مادون قرمز، بلوتوث، کیبردهای بی سیم و سایر ابزارهای انتقال اطلاعات بی سیم که امکان اتصال به سامانه ها را دارد، شبکه های بی سیم با امکان قرارگیری در معرض سو استفاده، ابزارهای چندکاره فکس، کپی، اسکن و... و همچنین تلفن ها و سامانه های تلفنی است.

به منظور کاهش تهدیدات آنها، شیلد کردن تجهیزات رادیویی و دارای تشعشع، قرار ندادن تجهیزات شبکه های بی سیم با برد بالا و امکان سواستفاده از آن، رمزنگاری اطلاعات در این بسترها و آگاهی کارکنان از خطرات و تهدیدات آنها و اعمال سیاست های امنیتی از جمله اقدامات موثر در این خصوص است.

12- **نیازمندی های الزامی چارچوب سیاست امنیتی ممانعتی**: به منظور مقابله با تهدیدات رایج امنیتی سایبری، 4 استراتژی برتر باید توسعه داده شود تا این استراتژی ها حملات هدفمند سایبری در اینترنت به شبکه ها و ایستگاه های کاری را کاهش دهد. این استراتژی ها در قالب یک چارچوب که به صورت لایه ای طراحی شده اند، در زیر نمایش داده شده است. این چارچوب لایه ای می تواند حداقل 85٪ حملات به ایستگاه های کاری در شبکه را پوشش دهد.



این چهار لایه از جمله مهمترین موارد در جلوگیری از حملات، اختلالات و نشت اطلاعات از ایستگاه های کاری در شبکه است. البته رعایت سایر موارد ممانعتی و جلوگیری کننده نیز به منظور افزایش سطح امنیتی الزامی است.

13- **محصول امنیتی**: استفاده از محصولات امنیتی که قابلیت لازم در کشف و جلوگیری از تهدیدات و آسیب پذیری های جدید داشته باشد، امری مهم است زیرا سازمان ها به منظور مقابله با تهدیدات و حفظ محرمانگی، اعتماد بسیاری به این محصولات می نمایند. بدین منظور باید محصولات امنیتی توسط مراجع ذیصلاح (مراکز و موسسات دارای فناوری و تخصص ارزیابی محصولات و اعطا گواهینامه رتبه بندی) ارزیابی و مورد تایید قرار گرفته و گواهینامه دریافت نمایند. سپس سازمان ها باید از میان آنها محصولات مورد نیاز خود را انتخاب نمایند.

انتخاب، تهیه و تامین، نصب و راه اندازی، تنظیم کردن، نگهداری، بهبود و استاندارد سازی و در نهایت جایگزینی یا حذف محصول، چرخه حیات یک محصول امنیتی است.

انتخاب یک محصول با اطمینان بالا، کمک بسیار زیادی به حفظ امنیت سازمان می کند لذا باید سازمان ها به هنگام استفاده از یک محصول، چرخه حیات آن را در نظر گرفته و زمانی اقدام به جایگزینی و حذف آن نمایند که یا دیگر نیاز سازمان نیست یا اطمینان و کارایی لازم را ندارد. به عنوان مثال بعضی سازمان ها اقدام به تغییر در فناوری خود نموده از سامانه ها و مکانیزم "ابر" استفاده می کنند، در این زمان بکارگیری فایروال و سامانه مدیریت یکپارچه تهدیدات مبتنی بر "ابر" الزامی

است یا رایانه کاربران تبدیل به ابزارهای موبایل و تبلت می شود که نیاز است محصولات امنیتی مانند ضدبدافزارها نیز تغییر نمایند.

14- **امنیت رسانه های ذخیره ساز**: امروزه خطرات بیشماری از سوی رسانه ها و ابزارهای ذخیره سازی و انتقال اطلاعات، سازمان ها را تهدید می کند.استفاده از یک برنامه که رسانه های ذخیره ساز و قابل اتصال به رایانه ها و شبکه ها را مدیریت و کنترل نماید، می تواند کمک قابل توجهی در جلوگیری از خروج و افشای اطلاعات نماید. فرآیندها، سیاست ها و روش های بهینه و مستندسازی آنها که به امنیت رسانه ها کمک نماید علاوه بر جلوگیری از استفاده سو از آنها در حال حاضر، می تواند جلوی تهدیداتی که در آینده متصور است را نیز بگیرد.

تهدید از اینجا ناشی می شود که وقتی سیستم عامل برای اجرای برنامه ای از روی رسانه مورد نظر، عملکردی را به صورت مجاز تلقی می کند، دیگر نمی تواند تفاوتی بین اجرای قانونی و درست و اجرای مخرب و نادرست آن قائل شود لذا سیستم عامل مورد تهدید واقع می شود. عامل مخرب می تواند از طریق آسیب پذیری های شناخته شده و با اتصال یک فلش به رایانه ای در شبکه، اطلاعات کلید رمز دسترسی به سایر سامانه ها را تخریب یا سرقت نماید. لذا ابزارهایی که به طور مستقیم به حافظه سیستم دسترسی دارند، می توانند عملیات خواندن یا نوشتن به حافظه را توسط عوامل مخرب انجام دهند لذا بهترین راه حل برای مقابله با تهدید این ابزارها، استفاده از ابزارهای کنترلی و یا خراب کردن فیزیکی پورت است تا نتوان ابزاری را به آن متصل نمود.

نتیجه:

در این مقاله به ارائه برخی از اصول پایه ای در امنیت اطلاعات از جمله امنیت فیزیکی، محصولات امنیتی، امنیت رسانه های ذخیره ساز، زیرساخت و ابزارهای ارتباطی پرداخته شد. رعایت و بکارگیری این اصول در امنیت اطلاعات توسط سازمان ها و شرکت ها و حتی افراد نقش چشمگیری را در مقابله با تهدیدات مختلف در فضای سایبر بازی می کند. باید توجه داشت که امنیت اطلاعات یک فرآیند است و به منظور مقابله با آسیب پذیری های فعلی و جدید باید این اصول را به عنوان یک راه حل یکپارچه و به هم پیوسته در نظر گرفت و از آنها استفاده نمود. در مقاله بعد سایر الزامات و اصول امنیت اطلاعات معرفی می گردد.

مراجع

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