**به نام خالق یکتا**

## اصول امنیت اطلاعات (اصول و قواعد پایه)

در ادامه مبحث ارائه شده در خصوص اصول امنیت اطلاعات که در مقاله قبل به معرفی برخی اصول پایه از جمله امنیت فیزیکی، محصولات امنیتی، امنیت رسانه های ذخیره ساز، زیرساخت و ابزارهای ارتباطی پرداخته شد، در این مقاله به معرفی و بررسی سایر اصول و قواعد امنیت اطلاعات، خواهیم پرداخت:

15- **امنیت نرم افزار**: نرم افزارها ممکن است دارای آسیب پذیری ها و حفره هایی باشند که توسط عوامل مخرب قابل بهره برداری شوند. این آسیب پذیری ها علاوه بر اینکه باعث دسترسی غیرمجاز به اطلاعات حساس و طبقه بندی می شود، ممکن است صحت و دسترس پذیری اطلاعات یک سازمان را هم تخریب کند یک مثال واقعی هدف قرار دادن وب سایت عمومی سازمان به منظور قطع دسترسی یا تغییر محتوای آن با اهداف بدخواهانه و سوء است.

**نصب و راه اندازی نرم افزار آنتی ویروس و فایروال های مبتنی بر نرم افزار که ترافیک ورودی و خروجی شبکه را محدود و کنترل می کند، نخستین گام موثر برای کاهش ریسک مخاطرات است.**

در حالی که امنیت نرم افزار در طول زمان توسط آسیب پذیری ها و اکسپلویت های جدید تنزل می یابد در نتیجه با اقداماتی همچون نصب آنتی ویروس و فایروال نرم افزاری به تنهایی نمی توان امنیت ایستگاه های کاری را حفظ کرد. اطمینان از به روز بودن وصله های سیستم عامل و نرم افزارها و همچنین نگهداری و مجهز کردن آنتی ویروس و سایر نرم افزار های امنیتی به آخرین امضای کدهای مخرب در مقابله با آسیب پذیری های شناخته شده کمک شایانی به امنیت ایستگاه های کاری می نماید.

باید توجه داشت که هر روزه آسیب پذیری های جدید و ناشناخته ای که به اصطلاح 0day هستند، در فضای سایبر منتشر می شود که توسط آنتی ویروس ها و سایر نرم افزارهای امنیتی قابل شناسایی نیستند لذا سازمان ها باید سازوکار لازم را برای مقابله با این کدها داشته باشد. محدود سازی در اجرای برنامه های کاربردی روی سیستم ها به عنوان برنامه های مجاز، کم کردن سطح دسترسی نرم افزارها به منابع، موجب افزایش امنیت و کاهش خطر انتشار و گسترش کدهای مخرب می گردد. این مساله به عنوان "فهرست سفید" برنامه های کاربردی معروف است. علاوه بر این محدود کردن انتشار اطلاعات درباره نرم افزارهای نصب شده در سازمان، می تواند یک کمک ویژه برای مقابله با خطر نفوذگرانی که به دنبال کشف نقاط حمله و بهره برداری از آسیب پذیری های نرم افزارها هستند، باشد.

بانک های اطلاعاتی دارای حجم وسیعی از اطلاعات هستند که به عنوان ثروت و سرمایه سازمان شناخته می شوند بنابراین به عنوان یک هدف مطلوب در حملات سایبری محسوب می شود چراکه با انجام یک عملیات هکری اطلاعات گرانبهایی در کمترین زمان در اختیار هکر قرار می گیرد. انتخاب کنترل ها و سیاست های امنیتی مناسب، ممیزی های

منظم و حذف تنظمیات پیش فرض و قرار دهی سرور بانک اطلاعاتی در لایه جداگانه و امن شبکه مختص بانک های اطلاعاتی، جلوی دسترسی غیرمجاز به این سیستم گرفته شده و ریسک ناشی از تجمیع اطلاعات کاهش می یابد.

**براساس آمار منتشره توسط موسسه وریزون، طی سال های 2011 تا 2013 برنامه های کاربردی رده دوم را از نظر از دست دادن اطلاعات و نقض امنیت دارا بودند.**

16- **امنیت ایمیل**: ایمیل ها به دلیل اینکه قادرند اطلاعات را به داخل و خارج سازمان منتقل نمایند به طور ذاتی متزلزل و ناامن هستند. امنیت ضعیف ایمیل ها باعث دسترسی آسان و غیرمجاز افراد به اطلاعات حساس و طبقه بندی شده سازمان که در ایمیل ها وجود دارد، می گردد. مهندسی اجتماعی از طریق ایمیل یکی از راه های رایج در انتقال کدهای مخرب به سازمان و آلوده کردن اهداف است. این تکنیک براساس بازکردن یک لینک مخرب یا فایل ضمیمه آن است.

هکرها از این تکنیک برای دستیابی به محل هایی استفاده می کنند که نمی توان به طور مستقیم و با روش های اکسپلویت مستقیم به آنها دست پیدا کرد. به منظور امن کردن ایمیل در برابر این تهدیدات و حملات مهندسی اجتماعی، پیاده سازی، مانیتورینگ، استفاده از تشخیص دهنده اسپم و نگهداری مناسب تنظیمات سرور ایمیل و برنامه کاربردی ایمیل از راه کارهای موثر هستند. اگرچه با استفاده از این تکنیک ها نمی توان قدرت بازدارندگی افراد سازمان را کاهش داد بلکه مهمترین راه حل، آموزش و اطلاع رسانی مناسب کارکنان است.

استفاده از چارچوب سیاست ارسال کننده(SPF) براساس فهرستی از آدرس های IP و امضاهای دیجیتال از دیگر راه کارهای مقابله با ایمیل های جعلی و مخرب است.

17- **کنترل دسترسی**: سازمان ها دسترسی به اطلاعات سامانه ها را از طریق کنترل دسترسی و محدود سازی متناسب اعمال می کنند. فرآیند کنترل دسترسی کاربران در سه مرحله شناسایی موفق کاربران، احراز هویت آنها و در نهایت اعطا و لغو مجوزهای دسترسی صورت می گیرد.

**براساس آمار منتشره سال 2012 توسط موسسه وریزون، 44٪ از رخنه اطلاعاتی، نتیجه بهره برداری از اطلاعات احراز هویت قابل حدس یا پیش فرض بوده است.**

ورود خودکار و سپس ممیزی اطلاعات مرتبط با فعالیت های شبکه می تواند احتمال کشف رفتار خطرناک را افزایش دهد. اختصاص یک شناسه کاربری یکتا به هر کاربر باعث ایجاد مسئولیت پذیری و پاسخگویی به رفتار کاربران می شود. همچنین استفاده از گواهی های کافی برای اطمینان از صحت یک کاربر، احتمال اعمال خطرناک را کاهش می دهد مثلا در حمله مهندسی اجتماعی به درخواست کلمه عبور مجدد (password reset) داشتن دو عامل مثل سوالات خاص و ایمیل اختصاصی یا شماره تلفن همراه برای شناسایی کاربر و ارسال کلمه عبور جدید الزامی است.

استفاده از کلمات عبور پیچیده و طولانی و غیرقابل حدس به عنوان سیاست انتخاب کلمه عبور که می تواند دروازه ورود و بهره برداری کاربران از سامانه های سازمانی باشد، برای ایجاد امنیت مناسب بسیار ضروری است. چراکه حملاتی مانند

brute force می تواند کلمات عبور 6 حرفی را در چند دقیقه بشکند. استفاده از احراز هویت چند عاملی نیز که حداقل از چند عامل مجزا مانند آنچه هست (بایومتریک)، آنچه دارد (توکن رمز شده و کارت هوشمند) و آنچه می داند(عبارت عبور) ترکیب شده باشد، در مقابله با حملات بسیار کارآمد است.

اصولا مجوزهای دسترسی در دو لایه قرار می گیرد. لایه اول مجوز دسترسی به سامانه قابل اتصال به اطلاعات و شبکه که شامل رایانه یا دسکتاپ مجازی یا ابزار موبایل است و لایه دوم نیاز به مجوزهای دسترسی به برنامه کاربردی مورد نظر، بانک اطلاعاتی یا منابع اطلاعاتی در آن سامانه است. استفاده از مکانیزم اعتبار سنجی، حفاظت مضاعفی را برای کاهش مخاطرات در یافتن و استفاده از اطلاعات توسط کاربری به ظاهر معتبر، بوجود می آورد. برای این کار نیاز است از مکانیزم اعتبار سنجی، لاگ گیری و ممیزی قوی جهت دسترسی به اطلاعات استفاده شود تا نفوذگر نتواند به راحتی خود را در قالب یک کاربر معتبر قرار داده و از منابع استفاده نماید. در لاگ گیری، داده های کافی باید نگهداری شود تا به کمک این داده ها در ممیزی آنها بتوان دسترسی های غیرمجاز و تخطی از هرگونه سیاست های امنیتی کشف گردد.

18- **مدیریت امن**: اداره کردن و مدیریت سازمانی امن به سازمان ها این امکان را می دهد که در مقابله با حملات سایبری به حساب های کاربری و دستگاه های حفاظت شده، بتواند نقش انعطاف پذیر، مقاوم و ارتجاعی را ایفا کند. اعمال کنترل های تکنیکی و تنظیمات شبکه منجر به بهبود امنیت اداره کردن آن می شود که نتیجه آن محدود کردن خرابی ها، پاسخگویی چالاک و سریع به رخدادها و تسریع در اقدامات بازیابی و درمان است. به منظور فعالیت های اداره کردن و مدیریت شبکه و دسترسی به دارایی های حیاتی استفاده از دستگاه و رایانه اختصاصی و جدا با امنیت بیشتری نسبت به سایر رایانه ها و همچنین داشتن شبکه با دسترسی اختصاصی برای انجام تنظیمات ابزارها، سخت افزارهای شبکه و سرورها، امری ضروری در ایجاد مدیریت امن است.

19- **رمزنگاری**: به منظور دستیابی کاربران مجاز و جلوگیری از دسترسی غیرمجاز به اطلاعات، رمزنگاری نخستین مانع است. رمزنگاری به منظور بهبود محرمانگی و حفاظت از اطلاعات حساس و طبقه بندی شده با ایجاد امکان غیرقابل خواندن برای غیرمجازها، پیشگام و بهترین اقدام است. علاوه بر اینها رمزنگاری می تواند در موارد زیر بسیار کمک کننده باشد:

- *صحت داده ها*: حفاظت از دستکاری تصادفی و عمدی اطلاعات با اطمینان از تغییر آنها
- *اجازه دسترسی*: اطمینان از هویت فردی که خودش ادعا می کند، به منظور محافظت از دسترسی به اطلاعات
- *عدم انکار*: اثبات انجام عملی توسط کاربر مانند ارسال یک پیام و جلوگیری از رد این موضوع توسط وی

باید به این نکته توجه داشت که حتی استفاده از رمزنگاری مورد تایید نتایج حملات موفق را کاهش نمی دهد در حقیقت هیچ محصولی در دنیا واقعی عاری از آسیب پذیری نیست. به منظور تایید رمزنگاری باید از الگوها و روش های ارزیابی الگوریتم های رمز که از نظر علمی و فنی می تواند در مقابل حملات مختلف کشف رمز ایستادگی کند، استفاده گردد. اگرچه همواره روش های ناشناخته و جدیدی می تواند صحت این الگوها را خدشه دار کند.

**طبق تحقیقات انجام شده در سال 2008 توسط مرکز منابع سرقت هویت، 82٪ از سازمان هایی که اطلاعات آنها به سرقت رفته اذعان داشتند که رمزنگاری، اطلاعات آنها را از خطر افشا حفظ کرده است.**

استفاده از هر محصول، الگوریتم یا پروتکل رمزنگاری به تنهایی برای کاهش خطرات احتمالی کافی نیست. الگوریتم و پروتکل تایید نشده و محصول رمزنگاری که به طور نامناسب تنظیم شده اند، موجب افزایش سطح ریسک می شوند. نصب یک برنامه با قابلیت رمزنگاری می تواند موجب افزایش محرمانگی اطلاعات طبقه بندی شده و حساس در هنگام ذخیره سازی و مبادله شوند. اگر این برنامه به طور صحیحی تنظیم و پیکربندی نشده باشد، ممکن است باعث کاهش امنیت جامع گردد.

در برخی مواقع رمزنگاری اثرات نامطلوبی نیز در امنیت می گذارد به عنوان مثال توانایی سازمان در بررسی ایمیل و ضمیمه رمزشده آن یا پویش فایل ها برای شناسایی ویروس و کد مخرب محدود می شود. بدین منظور باید توجه داشت که از الگوریتم هایی استفاده شود که مورد تایید باشد و همچنین در صورت مواجه با فایل های رمزنگاری متفرقه و تایید نشده از انتشار آنها جلوگیری به عمل آید.

رمزنگاری اطلاعات در هنگام ذخیره سازی موجب می شود که در صورت دسترسی فیزیکی و دستکاری تجهیزات محرمانگی حفظ شود همچنین رمزنگاری داده ها در هنگام انتقال و مبادله می تواند در مقابل استراق سمع، شنود و جعل اطلاعات نقش به سزایی ایفا نماید.

اطمینان از در دسترس بودن اطلاعات رمزنگاری از جمله کلید آن بسیار حائز اهمیت است چرا که در صورت بروز خرابی و از دست رفتن کلید رمزنگاری اطلاعات حساس بلا استفاده می گردند.

مدیریت مناسب سامانه رمزنگاری از جمله مدیریت کلید با بکاربستن مکانیزم حاکمیتی و شاخص های امنیت فیزیکی و کارکنان باعث حفظ صحت و محرمانگی اطلاعات می گردد.

20- **امنیت شبکه**: شبکه های سازمانی دارای اطلاعات و خدمات حیاتی کسب و کار، اطلاعات طبقه بندی شده و حساس هستند. نفوذگران سعی می کنند تا با بهره گیری از نقاط ضعف شبکه ها به اهداف خرابکارنه و دسترسی های غیرقانونی دست یافته و حتی اقدام به تغییر اطلاعات و خدمات نمایند. اگر فرصت دسترسی یک عامل مخرب به شبکه محدود شود، بنابراین فرصت تهدید شبکه کاهش می یابد. سازمان ها تلاش می کنند تا با ایجاد ساختار و تنظیمات مناسب، نقاط احتمالی دسترسی نفوذگران را کاهش دهند.

نکته مهم این است که به منظور کاهش آسیب پذیری های شبکه نه تنها شبکه های داخلی باید امن شوند بلکه شبکه های خارجی باسیم و بیسیم نیز باید از لحاظ امنیتی پایدار و مطمئن باشند. حتی ممکن است ابزارهایی که به شبکه های خارجی متصل می شوند به کدمخربی آلوده شوند که پس از جداسازی از شبکه خارجی به شبکه داخلی متصل گردند و این شبکه را نیز آلوده نمایند.

به منظور ایمن سازی شبکه اقدامات زیر ضروری است:

- *مدیریت جامع شبکه*: تمامی سیاست های امنیتی در تمامی بخش های شبکه های یکپارچه باید اعمال شود و آسیب پذیری ها شناسایی و حذف آنها با روش های مدیریت متمرکز شبکه در دست اقدام قرار گیرد، مستندسازی شبکه پس از هرگونه تغییرات ضروری بوده و از مکانیزم های جلوگیری و تشخیص نفوذ و مانیتورینگ و لاگ گیری فعالیت های شبکه استفاده شود.
- *طراحی و پیکربندی شبکه*: اجرای کنترل های دسترسی شبکه و کاهش نقاط دسترسی مانند غیرفعال کردن پورت های فیزیکی غیرقابل استفاده، پویش محتوا و فیلترکردن محتوای غیرضروری و اجرای کنترل دسترسی شبکه، امکان حملات را کاهش می دهد. سازمان ها باید مراقب اتصال ابزارهای خاص به شبکه باشند مانند نرم افزارهای کاربردی برای اجرای VOIP که ممکن است آسیب پذیری های اضافی را به شبکه تحمیل کند. در مورد شبکه های بیسیم، تفکیک شبکه، تغییر تنظیمات پیش فرض، فعال سازی احراز هویت و رمزنگاری و امن سازی ابزارهایی که برای اتصال به شبکه بیسیم استفاده می شوند، از جمله اقدامات مهم برای کاهش تهدیدات است.
- *زیرساخت شبکه*: کاهش پیچیدگی شبکه و جداسازی بخش ها به طور فیزیکی در شبکه تعداد نقاط دسترسی احتمالی را کم می کند. جداسازی فیزیکی و یا منطقی بخش های شبکه امکان دسترسی مهاجمان را از شبکه مورد تهاجم به سایر نقاط شبکه کاهش می دهد به عنوان نمونه در حملات DDOS که با ایجاد ترافیک غیرمتعارف و ناخواسته برای پایین آوردن سطح یا شکست خدمات انجام می شود، می توان جلوی بهره برداری از قربانیان سایر بخش های شبکه را گرفت. همچنین ایجاد لینک های اضافی و موازی موجب افزایش دسترس پذیری شبکه در هنگام حملات DOS یا رخدادهای احتمالی قطع ارتباط می شود. جداکردن بخش های شبکه رویکرد موثر دفاع در عمق را بوجود می آورد و برای هر بخش در صورت نیاز می توان مکانیزم های کنترلی و امنیتی جداگانه ای در نظر گرفت.

21- **امنیت دامنه های متقاطع**: اتصال یک دامنه امنیتی به دامنه امنیتی دیگر که شامل اتصال به اینترنت نیز هست، خطرات قابل توجهی را برای اطلاعات سازمان به همراه دارد. به عنوان مثال شبکه سازمانی با سیاست های امنیتی منحصر به فرد را به اینترنت که از نظر امنیتی در سطح پایین تری است، متصل گردد. همچنین اتصال شبکه دو بخش مختلف از سازمان یا دو سازمان شریک با شاخص ها و سیاست های امنیتی متفاوت جزء دامنه های امنیتی متقاطع محسوب می شود. مدیریت امن جریان داده در دروازه بین دامنه های امنیتی مختلف و اعمال تدابیر امنیتی می تواند این ریسک ها را کاهش دهد. بکار بردن تدابیر امنیتی شامل فیلتر کردن و فایروال محتوا در دروازه های سیستم و قرارگیری فیزیکی این مولفه ها در مکان مناسب ، خطر انتقال محتوای مخرب را به دامنه های مختلف کم می کند. همچنین قابلیت لاگ گیری و ممیزی به تشخیص رخدادهای امنیتی و اقدام متقابل با آن کمک می کند.

22- **انتقال داده و فیلترینگ محتوا**: هنگامی که داده ها از یک دامنه امنیتی به دیگری منتقل می شود خطر نشت اطلاعات به طور عمدی یا سهوی و دسترسی غیرمجاز به محتوا متصور است. دو اقدام می تواند به کاهش این ریسک کمک نماید:

- *اجرای سیاست انتقال داده*: اطمینان از جابجایی اطلاعات بین دامنه های امنیتی به صورت امن
- *بکاربردن فیلترینگ محتوا*: اجرای سیاست های امنیتی برای ورود و خروج اطلاعات و داده ها از یک دامنه امنیتی به منظور جلوگیری از ورود داده های مشکوک و مخرب و خروج داده هایی با محتوای حساس و طبقه بندی شده مانند استفاده از سامانه های DLP.

23- **کارکردن خارج از محل کار**: امروزه استفاده از ابزارهای موبایل در حوزه ارتباطات به امری الزامی و غیر قابل تفکیک از زندگی روزمره تبدیل شده است. با استفاده از ابزارهای موبایل، کارکنان می توانند به ایمیل، اینترنت و هر سامانه سازمانی که اجازه برقراری اتصال از راه دور فراهم شده باشد، از خانه، فرودگاه، هتل و... دسترسی داشته باشند. این فناوری دسترسی آسانتر، قابلیت جابجایی، سهولت در کاربری و افزایش کارایی را به همراه دارد. زمانی که یک سازمان از این فناوری استفاده می کند باید ریسک های آن را ارزیابی کرده و بپذیرد. هنگامی که یک دستگاه موبایل از محیط کنترلی سازمان خارج می شود، دیگر تحت حفاظت آن محیط نیست لذا علاوه بر مزایای قابلت جابجایی و کارکردن در خارج از محل کار، ریسک های جدیدی را برای سازمان به همراه دارد. بیشتر از آنچه که ابزارهای موبایل به کمک کاربران و استفاده از داده ها می آیند، نفوذگران می توانند با دستکاری آنها از منابع استفاده بیشتری نمایند.

کنترل ضعیف ابزارهای موبایل خصوصا دسترسی به سایت ها و ایمیل های مبتنی بر وب تهدیدات بیشمار اینترنتی از جمله کدهای مخرب، سرقت کلمات عبور و فایل های حساس را به همراه دارد. کارکنان سازمان به طور سهوی ابزارهای موبایل را به شبکه های سازمانی متصل می کنند که تهدیدات وسیعی را برای شبکه ها به همراه دارد. سازمان ها با اجازه دادن به کارکنان خود برای استفاده از ابزارهای موبایل ریسک بالایی را متحمل می شوند چرا که این ابزارها از کنترل های امنیتی در نظر گرفته شده برای سازمان مانند کنترل های احراز هویت و رمزنگاری بهره نمی گیرند.

وقتی کارکنان از این ابزارها هم برای اهداف شخصی و هم سازمانی استفاده می کنند بنابراین صرفا از قواعد و رفتارهای سازمانی تبعیت نمی کنند به عنوان مثال در هنگام مرور وب سایت ها، روی لینک های ناشناخته کلیک کرده و سایت های ناآشنایی را مشاهده می کنند که ممکن است کدهای مخرب را منتشر کنند. وقتی یک موبایل برای شارژ به رایانه ای متصل می شود امکان انتقال محتوای موبایل به رایانه وجود دارد که ممکن است باعث انتقال کدهای مخرب به رایانه شود.

حفظ حریم خصوصی از دیگر مواردی است که به هنگام استفاده از این ابزارها برای اهداف کسب و کار باید مدنظر قرار گیرد.

براساس گزارش شرکت سیمنتک، تعداد آسیب پذیری های موبایل بین سال های 2011 تا 2012 بیش از 25٪ افزایش یافته است و باید در نظر داشت که ریسک استفاده از ابزارهای موبایل برای اهداف سازمانی و کسب و کار بیشتر از فواید و مزایای آن است.

جهت کاهش مخاطرات ناشی از ابزارهای موبایل باید سیاست هایی را برای محافظت از این ابزارها توسعه داد که توسط کاربرانشان در خارج از محیط کار و تسهیلات کنترلی و امنیتی قابل اجرا باشند و در حقیقت کارکنان هنگام کار در منزل یا خارج از محیط کار با امکانات امنیتی مشابه محیط کاری سروکار داشته باشند.

به منظور کاهش خطرات ناشی از ابزارهای موبایل اقدامات زیر ضروری است:

- *کاربری قابل قبول*: با تهیه و ابلاغ سیاست های امنیتی خاص برای کارکنان و آگاهی آنها از نحوه استفاده از ابزارهای موبایل در محیط های مجاز و غیرمجاز و اطلاع از نوع محتوای قابل انتقال و ریسک انتقال اطلاعات طبقه بندی شده می توان ریسک ناشی از استفاده ابزار موبایل را در دو محیط متفاوت داخل و خارج سازمان کاهش داد.
- *تنظیمات امن موبایل*: از آنجایی که موبایل ها در خارج از محل کار نیز استفاده می شود براحتی در خطر سرقت و گم شدن قرار دارند. روش های انهدام اضطراری در صورت از دست دادن دستگاه می تواند جلوی نشت اطلاعات را بگیرد. رمزنگاری مناسب اطلاعات در هنگام ذخیره سازی و انتقال نیز در افزایش امنیت تاثیرگذار است.
- *اتصالات و ارتباطات بیسیم*: شبکه های بیسیم به طور ذاتی امنیت فیزیکی شبکه های باسیم را ندارد و نفوذگر می تواند با فرصت بیشتری از راه دور به شبکه نفوذ کند. انتقال بیسیم اطلاعات از طریق فناوری های بیسیم، مادون قرمز و بلوتوث به شبکه های سازمانی محدود و حتی ممنوع است چرا که عامل مخرب می تواند به راحتی در آن اخلال ایجاد کرده و آنها را شنود نماید.
- *تعمیر و نگهداری*: به منظور حفظ محرمانگی و صحت اطلاعات ذخیره شده یا درحال انتقال روی یک ابزار موبایل از ممیزی ها و به روز رسانی امنیتی مستمر و منظم باید استفاده نمود. نرم افزارهای امنیتی باید به روز باشند. در تعمیرات موبایل ممکن است داده های حساس از آن به سرقت رفته یا حتی نرم افزارهای مخرب روی آن نصب شود لذا باید از تعمیرگاه های مورد تایید سازمان استفاده نمود.
- *کار در خانه*: به منظور کار در خانه و حارج از محل کار نباید از لینک های ضعیف و ناامن برای اتصال به سامانه های سازمانی استفاده نمود و پروتکل های مدیریت امنیت فیزیکی و چارچوب سیاست امنیتی ممانعتی را که در اصول قبلی به آن اشاره شده را رعایت نمود.

**نتیجه**:

در این مقاله به ارائه مابقی اصول پایه ای در امنیت اطلاعات از جمله امنیت نرم افزار، شبکه، رمزنگاری، موبایل، دامنه های متقاطع و مدیریت امن پرداخته شد. نکته مهم در بکارگیری این اصول، نیاز سازمان با توجه به ساختار شبکه، گستردگی، توسعه پذیری، انعطاف پذیری و سطح اشتراک اطلاعاتی و از همه مهمتر اهمیت اطلاعات و دارایی های سازمانی است. باید توجه داشت که سازمان ها باید این اصول را در تمامی شبکه های خود اجرا و بکارگیری نمایند. در برخی مواقع بنگاه های مختلف، شرکت ها و سازمان ها با یکدیگر همکاری و شراکت می کنند یا حتی ادغام می شوند در این حال نیاز است که پروتکل ها و سیاست ها، چارچوب ها و اصول امنیتی مشترکی تدوین گردد و از یک اصول واحد در امنیت اطلاعات بهره برداری نمایند. این قواعد باید نیازهای امنیتی هر سازمان و نیازهای مشترک آنها را پوشش

دهد و اصول امنیتی بیان شده در این مقاله می تواند منبع ارزشمندی برای طراحی، پیاده سازی و اجرای چارچوب امنیتی توسط کارشناسان و متخصصین شبکه و امنیت اطلاعات در این سازمان ها باشد.

## مراجع


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

VERIZON. (2014). *DATA BREACH INVESTIGATIONS REPORT.* VERIZON.