تاریخ دریافت:۱۳۹۴/۱۱/۱۰
تاریخ پذیرش: ۱۳۹۵/۰۳/۱۳

فصلنامه علوم و فنون نظامی/ سال یازدهم/ شماره ۳۲، تابستان، ۱۳۹۴
صص ۷۹-۵۳

شیوه‌های مناسب مقابله اطلاعاتی آجا در برابر تهدیدهای امنیتی نیروهای فرامنطقه‌ای

علی رستمی [۱]

چکیده

هدف این پژوهش بررسی و یافتن مناسب‌ترین شیوه و شگردهای مقابله اطلاعاتی آجا در برابر نیروهای فرامنطقه‌ای می‌باشد. براساس مطالعه منابع مختلف و رویکردهای نیروهای فرامنطقه‌ای در دنیای ارتباطات نوین فضای جامعه جهانی را به صورت یک دهکده تحت کنترل خود در آورده و بخش عمده‌ای از ارتباطات اطلاعاتی، نظامی، امنیتی، فرهنگی، اقتصادی‌و... را به سمت فضای سایبری سوق داده با این شیوه اهداف شوم خود را در جنگ اطلاعاتی به صورت آشکار و پنهان و نامحسوس از طریق این ارتباطات دنبال می‌نماید. در چند دهه‌ی گذشته در عرصه‌های مختلف اطلاعاتی مشکلات و تهدیدات جدی را بر علیه نظام جمهوری اسلامی از جمله آجا ایجاد نمودند. بنابراین ضرورت دارد که از شیوه‌های مختلف مقابله‌ای بهره برداری مؤثری صورت بگیرد. سازمان حفاظت و اطلاعات باید اطمینان پیدا کند که کلیهی فرایندهای سازمانی منطبق بر سیاست امنیت اطلاعات و استانداردهای امنیت اطلاعات انجام می‌گیرد. در این مقاله که به شیوه تحلیلی – توصیفی انجام می‌شود تلاش شده است شیوه‌های مقابله‌ای و بازدارنده اطلاعاتی را با تاکیده بر استانداردهای فنی و مدیریت امنیتی مورد بررسی قرار گیرد.

واژگان کلیدی

استاندارد فنی، مدیریت امنیت، مقابله اطلاعاتی، نیروهای فرامنطقه

[۱]- کارشناس ارشد مدیریت دفاعی دانشگاه فرماندهی و ستاد تلفن: ۶۶۴۱۲۲۲۹-۰۲۱

مقدمه

الگوی نبردها در قرن جدید، الگوی کاملاً متفاوت با دهه‌های گذشته است. هدف جنگ‌های نوین متحول شده و دولت‌ها و یا سازمان‌ها و گروه‌های تروریستی با اهداف متنوع و متعدد و متفاوت از گذشته به جنگ می‌پردازند و هم روش‌های رزم نوین با توجه به ورود سیل عظیم تکنولوژی‌های برتر به عرصه نظامی، تغییر یافته است. مطالعه روند تحقیقات نظامی کشورهای غربی بیانگر این واقعیت است که چالش جدیدی به نام جنگ‌های اطلاعاتی به وجود آمده است. جنگ نیروهای فرامنطقه‌ای علیه عراق و ... به وضوح این پیام را در بر داشت که رویارویی بسیاری از کشورهای جهان با قدرت‌های نظامی، غیرمنطقی بوده و نبردی نابرابر را در پی خواهد داشت. از طرفی با روند سرسام‌آور توسعه‌ی فناوری‌های اطلاعاتی و قابل دسترس بودن آن برای همگان و نیز آسیب پذیری شدید کشورهای غربی از طریق شبکه‌های ارتباطی و اطلاعاتی، این گمان که اگر رویارویی با نیروهای فرامنطقه‌ای با روش‌های متعارف مقدور نباشد، صدمه زدن به آن‌ها از طریق جنگ‌های اطلاعاتی غیرممکن نخواهد بود و لازم است به ابعاد مختلف جنگ‌های مدرن یا جنگ‌های اطلاعات مدار پرداخته شود. ارتش ج.ا.ا نیز از قاعده بالا مستثنی نمی‌باشد و تهدیدات نوینی که امنیت ملی ج.ا.ا را نشانه رفته‌اند، الزاماً همان تهدیدات سابق نیستند و نیازمند پی‌ریزی یک راهبرد و تاکتیک‌های دفاعی نوینی هستند. جنگ‌های امروزه مبنای اصلی‌شان بر اطلاعات است و می‌توان به جرأت گفت که بیشتر جنگ‌های امروزی، جنگ در عرصه اطلاعات است تهدیداتی که از ناحیه آسیب‌پذیری‌های اطلاعاتی متوجه یگان‌های رزمی آجا است، هر چه بیشتر ضرورت تدوین الگویی عملی و مناسب را جهت نبردی احتمالی در آینده آن هم به شیوه نامتقارن و با قدرتی برتر و بزرگ‌تر، یادآوری می‌نماید. هفت نوع از انواع رویارویی اطلاعاتی با عناوین جنگ از جمله فرماندهی و کنترل، هوشمندی تجهیزات، جنگ الکترونیک، عملیات روانی، سایبریک، حفاظت از اطلاعات نظامی و فریب اطلاعاتی در فضای مجازی از جمله مواردی است که در آجا باید مورد بحث و بررسی قرار گیرد. تبیین سناریو نبردهای اطلاعاتی بر اساس نبردهای اطلاعات مدار از مهم‌ترین عوامل مؤثر به منظور رویارویی مؤثر با تهدیدات آینده بشمار می‌رود.

از این رو، پژوهش حاضر قصد دارد فهم نبرد اطلاعاتی مدار در محیط آجا را مورد کاوش قرار دهد. و با مطالعه و بررسی بر آسیب‌پذیری‌ها و تهدیدهای اطلاعاتی و امنیتی موجود در واحدهای رزمی آجا در نبرد احتمالی در آینده و شناخت نقاط ضعف و آسیب‌پذیری امنیتی

احتمالی در واحدهای رزمی و با توجه به تجربه جنگ‌های اخیر در منطقه شیوه‌های مناسب در مقابله با تهدیدهای امنیتی احتمالی و آینده در محیط اطلاعاتی را تبیین نماید. بنابراین سؤالاتی که در این تحقیق پاسخ داده می شود عبارتست از: اولاً: مناسب‌ترین شیوه‌های مقابله اطلاعاتی ساحفاجا با استفاده از استانداردهای فنی امنیت در برابر تهدیدهای امنیتی نیروهای فرامنطقه‌ای کدامند؟ و در ثانی مناسب‌ترین شیوه‌های مقابله اطلاعاتی ساحفاجا با استفاده از استانداردهای مدیریتی امنیت در برابر تهدیدهای امنیتی نیروهای فرامنطقه‌ای کدامند؟

حفاظت از اطلاعات

در جنگهای نسل پنجم و ششم ماهیت حملات به گونه ای است که زیرساخت نامرئی و نا شناخته را برای عامه جامعه را مورد هدف قرار می دهد در این نوع حملات عمدتا یک شبکه رایانه‌ای که حاصل پیوند سه عنصر مهم سرویس‌های فعال، پروتکل‌های استفاده شده و پورت‌های باز (درگاه) می‌باشد و کارشناسان امنیت اطلاعات را که با تمرکز بر سه محور فوق، شبکه‌ای ایمن و مقاوم در مقابل انواع حملات را ایجاد و نگهداری نمایند؛ مورد حمله قرار می‌دهد. به عبارتی ایجاد اختلال در منابع و یا از کار انداختن سرویس‌هایی که کاربران قصد دست‌یابی و استفاده از آنان را دارند مهم‌ترین هدف این نوع از حملات به منظور سلب دست‌یابی کاربران به یک منبع خاص است. و مهاجمان با بکارگیری روش‌های متعددی تلاش می‌نمایند که کاربران مجاز را به منظور دست‌یابی و استفاده از یک سرویس خاص، دچار مشکل نموده و به نوعی در مجموعه سرویس‌هایی که یک شبکه ارائه می‌نماید، اختلال ایجاد نمایند. تلاش در جهت ایجاد ترافیک کاذب در شبکه، اختلال در ارتباط بین دو ماشین، ممانعت کاربران مجاز به منظور دست‌یابی به یک سرویس، ایجاد اختلال در سرویس‌ها، نمونه‌هایی از سایر اهدافی است که مهاجمان دنبال می‌نمایند مقابله با این نوع تهدیدهای اطلاعاتی شناخت و ارزیابی تهدید در اولین گام باید موارد زیر را مدنظر قرار دهد: شناخت صحیح و دقیق تهدید، ارزیابی توان و ظرفیت‌های تهدید و اندازه‌گیری خطر ناشی از وقوع تهدید امری اساسی است با این رویکرد، ایمن‌سازی اطلاعات حفاظتِ از اطلاعات و نظام‌های اطلاعاتی در مقابل حملات کارکنان، اطلاعات، اسناد و مدارک، اماکن، تأسیسات، وسایل و تجهیزات و ارتباطات مخابراتی را از فعالیت‌های جاسوسی، براندازی، خرابکاری و

نفوذ جریانات سیاسی حفظ و صیانت نموده و از موارد ایجاد نارضایتی و اختلال در اجرای مأموریت‌های آجا جلوگیری می‌نماید. (جهانگیری، ۲۵:۱۳۷۹)

استانداردسازی مدیریت امنیت

استاندارد نظمی است مبتنی بر نتایج استوار علوم، فنون و تجارب بشری در رشته‌ای از فعالیت‌های عمومی که به صورت قواعد، مقررات و نظام نامه به منظور ایجاد هماهنگی و وحدت رویه، توسعه تفاهم، تسهیل ارتباطات، صرفه جویی در اقتصاد، حفظ سلامت و گسترش مبادلات بازرگانی داخلی و خارجی بکار می‌رود. (لشینسکی،۱۷:۱۳۹۰) استاندارد مدیریت امنیت هم از همین قاعده پیروی می‌کند، استانداردسازی مدیریت امنیت ویژگی است که توانایی بخشیدن به یک سازمان برای طراحی، پیاده‌سازی، نگهداری و پشتیبانی یک مجموعه پیوسته از فرآیندها و سیستم‌ها که فرآیندها و سیستم‌های مذکور که سطح قابل قبولی از امنیت اطلاعات شامل محرمانگی، تمامیت و در دسترس بودن را فراهم کنند. (همان: ۱۹)

از این رو در یک سامانه اطلاعاتی، داده‌ها از جنبه‌های مختلف مانند خطاهای کاربر، حملات بدخواهانه و غیر بدخواهانه و ... در معرض خطر می‌باشند. ممکن است مهاجمان از راه‌های مختلف به این سامانه‌ها دسترسی پیدا کرده، سرویس‌ها را مختل یا بدون استفاده سازند و یا اطلاعات آن‌ها را تغییر داده و حذف یا سرقت نمایند. بنابراین سامانه‌های اطلاعاتی جهت حفاظت از داده‌ها، باید شامل موارد زیر باشند.

محرمانگی[1]: اطلاعات و منابع رایانه‌ای، سری بوده و نباید در دسترس افراد تأیید نشده قرار گیرد و تنها کسانی مجاز به دسترسی و استفاده از آن می‌باشند که مورد تأیید مراجع ذی‌صلاح قرار گیرند.

جامعیت[2]: حفظ جامعیت به معنای حفاظت داده‌های سیستم در مقابل تغییرات غیر مجاز سهوی یا عمدی است. برای حفظ جامعیت، برنامه امنیتی باید همواره اطلاعات را در حالتی که مورد انتظار کاربران سیستم است، نگه دارد. به بیان دیگر منابع و اطلاعات رایانه‌ای بین دو کاربر باید به طور صحیح و بدون تغییر در محتوا یا دست‌کاری آن‌ها مبادله گردند و به جز افراد مجاز، هیچ کس مجاز به تغییر آن‌ها نمی‌باشد.

1 . Confidentiality
2. Integrity

دسترس پذیری[1]: اطلاعات باید همیشه در دسترس افراد مجاز باشد تا به راحتی بتوان به آن‌ها دسترسی پیدا کرد.

امنیت فناوری اطلاعات و ارتباطات

فناوری اطلاعات از گردآوری، سازماندهی، ذخیره و نشر اطلاعات اعم از صوت، تصویر، متن یا عدد که با استفاده از ابزار رایانه‌ای و مخابراتی صورت پذیرد (علی احمدی،۶۸:۱۳۸۳) فناوری ستون فقرات ارتباطی فناوری اطلاعات و در واقع شاه‌راه ساختار فناوری اطلاعات را تشکیل می‌دهد؛ و بستر مخابراتی لازم برای انتقال فیزیکی اطلاعات در حوزه عملکرد فناوری اطلاعات می‌باشد و آسیب و تهدید در این حوزه منابع حیاتی یک سیستم را تهدید می‌کند. بنابراین امنیت در حوزه فناوری اطلاعات به حفاظت از اطلاعات و به حداقل رساندن خطر افشای اطلاعات در بخش‌های غیرمجاز ممکن می‌سازد. امنیتفناوری اطلاعات و ارتباطات از ابزارها برای جلوگیری از سرقت، حمله، جنایت، جاسوسی و خرابکاری و علم مطالعه روش‌های حفاظت از داده‌ها در رایانه‌ها و نظام‌های ارتباطی در برابر دسترسی و تغییرات غیرمجاز محافظت می‌کند (احمدی،۱۳۸:۱۳۸۳) با توجه به مباحث اشاره شده، امنیت فناوری اطلاعات و تدابیر، روش‌ها و ابزارها برای جلوگیری از دسترسی و تغییرات غیرمجاز در نظام‌های رایانه‌ای و ارتباطی مورد توجه قرار می دهد در یک نگاه ساده روش مناسب پیشگیری از حملات رایانه‌ای، آموزش کاربران و مانیتورینگ عملکرد هر یک از نرم افزارهای موجود باشد منابع و سایت‌های مطمئن اقدام به دریافت و نصب نرم‌افزار بر روی سامانه‌ی مورد استفاده نمایند

بدیهی است در این روند سخت‌افزار، نرم‌افزار و داده، منابع اصلی هر سامانه رایانه‌ای می‌باشند. چهار نوع تهدید، علیه این منابع وجود دارد: هر یک از منابع به شکلی که در جدول زیر نشان داده شده است، در مقابل بعضی از تهدیدات، آسیب پذیر هستند.

1. Availability

جدول ۱) رابطه تهدیدات و منابع

تهدیدات / منابع	وقفه	جلوگیری	تغییر	ساخت
سخت افزار	✓	✓	–	–
نرم افزار	✓	✓	✓	–
داده	✓	✓	✓	✓

در تحلیل امنیت اطلاعات و ارتباطات نکته ای بسیار مهم می‌باشد امنیت نرم‌افزاری است امنیت سخت افزاری معمولا با ندابیری از قبیل محدودیت منع دسترسی محافظت فیزیکی و سایر تدابیر بهتر مراقبت میگردد اما امنیت نرم افزاری نیازمند دانش، ترفندها، کدها غیرقابل دسترس می باشد. رایانه‌ها چه از جنبه‌های سخت‌افزاری و چه از جنبه‌های نرم‌افزاری قابلیت محافظت از خود را دارند، چنانچه در برنامه‌ها یا نرم افزارها به اندازه کافی به مسائل امنیتی توجه شده باشد، رایانه‌ها با اجرای چنین نرم‌افزارهای امنی از خود و اطلاعات ذخیره شده محافظت خواهند نمود و این امر نقش مهمی در اعمال شیوه‌های امنیتی مراکزی دارد که دارای سیستم‌های رایانه‌ای هستند. هرچه برنامه‌ها و سیستم‌ها، پیچیده‌تر و بزرگ‌تر باشند نیاز به اعمال شیوه‌های کنترل دسترسی و ایمن‌سازی نرم‌افزارها بیشتر احساس می‌شود.

گسترش روزافزون استفاده از رایانه‌های شخصی و دسترسی آسان به شبکه‌های رایانه‌ای نیز، بر ضرورت تهیه و اجرای برنامه‌هایی که به نکات ایمنی توجه لازم و کافی را مبذول داشته باشند، می‌افزاید. معیارهای سنجش میزان ایمنی سیستم بایستی به گونه‌ای طراحی شوند که اجزای سخت‌افزاری و نرم‌افزاری هر یک به طور جداگانه قابل بررسی باشند. طراحی صحیح نرم‌افزار در کنترل انواع اطلاعاتی که کاربر مجاز است به آن دسترسی داشته باشد، نقش مهمی ایفا می‌کند.

بنابراین، فعالیت‌های امنیتی نیز نیازمند به روز شدن و تجدید نظر هستند. این تغییرات به طور معمول وقتی نیاز به تغییرات عمده پیدا می‌کنند که پیکربندی و دیگر شرایط و وضعیت‌ها به صورت برجسته تغییر کنند یا سیاست‌ها و قواعد سازمانی متحول شوند.

چند نمونه از سیاست‌های احتمالی امنیت عبارتند از:

سیاست‌های امنیتی فیزیکی، مانند کنترل‌های دسترسی فیزیکی

سیاست‌های امنیتی شبکه، مانند سیاست‌های پست الکترونیکی و اینترنتی

سیاست‌های امنیتی داده، مانند کنترل دسترسی و کنترل صحت

برای هر یک از سیاست‌ها باید نوعی راهبرد بازدارنده در کنار یک راهبرد واکنشی وجود داشته باشد. راهبرد بازدارنده یا پیش از حمله، به کاهش آسیب‌پذیری کمک می‌کند و خسارات، ضعف‌ها و نقاط آسیب‌پذیری در یک حمله را مورد بررسی قرار داده، به توسعه راهبرد واکنشی کمک می‌کند.

راهبرد واکنشی، خسارات ایجاد شده در یک حمله را بازسازی و راهبرد بازدارنده را تکمیل، مستندسازی و تجربه کرده و آن را به خاطر می‌سپارد.

برای ارزیابی امنیت یک سامانه، باید انواع تهدیدها را در آن، مورد بررسی قرار داد. تهدیدها انواع مختلفی دارند. به عنوان مثال قطع برق می‌تواند به عنوان یک تهدید در سامانه باشد که منجر به از دست رفتن اطلاعات شود و برای مقابله با آن باید سامانه حفاظتی‌ای طراحی کرد. یا کارمند ضعیف و نالایقی که ممکن است با سهل‌انگاری خود موجب از دست رفتن اطلاعات یا لو رفتن آن شود، اخراج کرد.

بحث و تجزیه و تحلیل یافته‌ها

سیاست امنیتی لایه‌ای

با توسعه فن‌آوری اطلاعات و پیاده سازی سیستم‌های اطلاعاتی در سراسر دنیا، تأمین امنیت آن به عنوان دغدغه‌ای مهم در مجامع علمی و دولتی مطرح شده است. از آنجا که شبکه به عنوان بستری اساسی برای انتقال اطلاعات به حالتی فراگیر نزدیک شده است، حفظ امنیت در انتقال اطلاعات و عدم نفوذ پذیری از طریق شبکه، به عنوان حالتی خاص از امنیت اطلاعات، نیاز به بررسی بسیار دارد و آشنایی مدیران سازمان‌ها، مراکز دولتی و به خصوص نظامی که امنیت اطلاعات برای آن‌ها از اهمیت بالاتری برخوردار است، با مبانی امنیت شبکه، مخاطرات امنیتی، راه‌حل‌ها و نحوهی سیاست‌گذاری صحیح برای این موضوع، امری اجتناب ناپذیر محسوب می‌شود (بیژنی، ۱۳۸۳: ۳۸). بنابراین برای امنیتی سازی شبکه‌ها سیاست لایه‌ای در سیستمهای حفاظتی و امنیتی اتخاذ می‌گردد[۱]

[۱]- این گونه سیاست‌ها به سیستمهای نظامی اختصاص ندارد و در بیشتر سیستمهای امنیتی و شرکتهای تجاری که نیازمند حفظ اطلاعات و داده های خود می باشند؛ بکار گرفته می شود .

لایه اول: امنیت فیزیکی

معین کردن اینکه چه کسی اجازه نصب، برداشتن و جابه‌جایی مسیریاب را دارد.

مشخص کردن اینکه چه کسی اجازه نگهداری و تغییر در سخت‌افزار و پیکربندی فیزیکی مسیریاب را دارد.

معین کردن اینکه چه کسی اجازه برقراری ارتباط فیزیکی با مسیریاب را دارد.

تعریف کنترل روی دسترسی به درگاه‌های فیزیکی و کنسول مربوط به مسیریاب.

مشخص کردن روند انجام تعمیرات فیزیکی مسیریاب. (سادوسکای، ۲۰۱۱)

لایه دوم: امنیت نرم افزار و پیکربندی ثابت:

معین کردن اشخاصی که اجازه ورود مستقیم به پیکربندی مسیریاب از طریق پورت‌های مستقیم، از جمله درگاه کنسول را دارند.

مشخص کردن کسانی که حق مدیریت مسیریاب را دارند و تعریف حقوق مشخص آن‌ها.

تعیین روش‌های تغییر در پیکربندی ثابت.

تعریف سیاست مربوط به رمزهای عبور مربوط به مدیران و سطوح امنیتی مختلف مسیریاب. همچنین شرایطی که تحت آن باید رمزهای عبور تغییر داده شوند.

معین کردن افرادی که حق دسترسی و ورود از راه دور به مسیریاب را دارند.

مشخص کردن روش‌های دسترسی از راه دور.

معین کردن روش‌های مدیریت خودکار و ابزار کنترل مسیریاب و محدودیت‌های آن.

معین کردن روش‌ها و تدوین راهنمایی‌هایی برای کشف و مقابله با حملات.

لایه سوم: پیکربندی پویا:

تعریف سرویس‌های اجازه داده شده برای پیکربندی پویا و شبکه‌ها یا دستگاه‌هایی که مجوز این کار را دارند.

مشخص کردن پروتکل‌های مسیریابی‌ای که استفاده می‌شود و امنیت آن‌ها.

لایه چهارم: امنیت داده‌های عبوری و سرویس‌ها

مشخص کردن پروتکل‌ها، پورت‌ها (پورت نرم‌افزاری) و سرویس‌هایی که اجازه عبور دارند یا باید از آن‌ها جلوگیری شود. با ذکر واسط مربوطه و نوع آن.

توصیف روش‌های به دست آوردن سرویس‌های تعیین شده در بالا و روش‌های نگه‌داری آنها (بیژنی و کرامتی، ۱۳۸۳: ۲۶).

استانداردهای موجود برای صحت امنیت نرم افزاری

گستره آسیب‌پذیری‌ها بسیار متنوع است و می‌تواند از امنیت فیزیکی ضعیف شبکه‌ها تا خطاهای ناشناخته نرم‌افزاری را شامل شود. در اکثر اوقات مدیریت ضعیف، باعث آسیب‌پذیری سامانه می‌شود. اداره ضعیف یک سامانه، مشکلی عمومی است که وقتی در کنار آسیب‌پذیری‌های دیگر قرار گیرد، بسیار خطرناک خواهد شد. رشد روز افزون به کارگیری شبکه‌های رایانه‌ای از یک سو و ماهیت توزیع شده و عدم امکان کنترل مرکزی در شبکه‌ها از سوی دیگر سبب شده تا تأمین امنیت شبکه‌های رایانه‌ای از اهمیت ویژه‌ای برخوردار شود. همچنین وجود مشکلات امنیتی در پروتکل‌های شبکه و در دسترس بودن مشخصات این پروتکل‌ها و بعضاً کد پیاده‌سازی شده آن‌ها باعث بروز ناامنی‌های بسیاری در شبکه‌های عمومی شده است. بر همین اساس مطابق استانداردی که توسط وزارت دفاع آمریکا تهیه شده است، امنیت یک سامانه رایانه‌ای به رده‌های زیر دسته‌بندی شده است:

کلاس	مشخصه کلاس	کلاس	مشخصه کلاس
D1	فاقد هر نوع سیستم امنیتی	C1	گروه بندی کاربرانی که در یک سطح امنیتی هستند، کافی است که کاربران و اطلاعات مربوطه از هم جدا شوند
C2	هر کاربری جداگانه شناخته شده باشد، از مکانیزم تصدیق برای ورود به سیستم و محیط هر کاربر استفاده می‌شود	B1	کنترل دسترسی اجباری است همه راه‌های شناخته شده‌ی ورود به سیستم رفع شده است مشخصه رسمی یا غیر رسمی مدل امنیت، قابل دسترسی است. وظایف مدیر سیستم کاملاً تعریف شده است.
B2	در این کلاس علاوه بر قواعد کلاس B1 موارد امنیتی زیر نیز رعایت می‌شود. ایجاد کنترل دسترسی اجباری به تمام اجزایی که مستقیم یا غیر مستقیم در سیستم اطلاعاتی در دسترس است. مسیر ارتباط بین کاربران و سیستم اطلاعات باید امن باشد (امنیت خطوط ارتباطی). سیستم اطلاعات باید از تشعشع امواج الکترومغناطیسی در امان باشد. وظایف مدیر و اپراتور باید از هم جدا شود. باید مشخصات رسمی برای مدل امنیت شبکه وجود داشته باشد. حداقل و حداکثر محرمانگی کارها و ابزارها مشخص شود.	B3	علاوه بر ویژگی‌های کلاس B2 دارای موارد زیر نیز می‌باشد. لیست دسترسی باید شامل اسامی و کاربران غیر مجاز نیز باشد. مشخصات کاری سیستم اطلاعات با جزئیات بسیار دقیق وجود داشته باشد. سیستم اطلاعاتی باید به صورت پیمانه‌ای طراحی شده باشد. بعضی از پیاده‌سازی‌ها باید در سطح سخت‌افزاری طراحی شود. مکانیزم‌های تضمینی بعد از رخداد مساله‌ای باید سیستم را به حالت واقعی نگه‌دارند.
A1	علاوه بر ویژگی کلاسهای دیگر دارای مشخصات طراحی نرم افزار رسمی است		

سامانه تشخیص هویت مبتنی بر شبکه[۱]

نام NIDS از این حقیقت مشتق شده است که از منظر محلی که قرار گرفته، بر تمام شبکه نظارت دارد. شناسایی و تشخیص نفوذهای غیرمجاز قبل از رسیدن به سیستم‌های بحرانی، به عهدهی سیستم تشخیص نفوذ مبتنی بر شبکه است. سیستم‌های تشخیص نفوذ مبتنی بر شبکه اغلب از دو بخش ناظر (حسگر) و عامل تشکیل شده‌اند. این دو بخش اغلب در پشت دیوارهی آتش و بقیهی نقاط دسترسی برای تشخیص هر نوع فعالیت غیرمجاز نصب می‌شود. عامل‌های شبکه می‌توانند جایگزین زیرساختار شبکه شوند تا ترافیک شبکه را جستجو کنند. نصب عامل‌ها و ناظرها این مزیت را دارد که هر نوع حمله‌ای را در ابتدا از بین می‌برد. ضمناً دنباله‌های بررسی یک یا چند میزبان می‌توانند برای جستجوی علائم حملات، مفید باشند. سیستم‌های تشخیص نفوذ مبتنی بر شبکه نیاز به کلمهی عبور برای برنامه‌های کاربردی، حقوق مربوط به سیستم عامل شبکه یا اتصالات مربوط به سیستم در هنگام اجرای نرم افزار ندارد. همچنین از آنجا که این سیستم‌ها در سطح لایهی شبکه عمل می‌کنند، به سیستم‌عامل وابستگی ندارند. ضمناً هیچ‌گونه سربار و تغییری روی سرویس‌دهنده‌ها و ایستگاه‌های کاری به وجود نمی‌آورند، چرا که برای این سیستم‌های تشخیص نفوذ نیازی به نصب ابزارهای اضافی نیست.

سامانه هویت سنجی برای پیشگیری از نفوذ[۲]

سیستم‌های پیشگیری از نفوذ که به اختصار IPS نامیده می‌شوند، سیستم‌های بازدارنده‌ای هستند که به منظور تشخیص بسته‌های خطرناک در داخل ترافیک معمولی (عملیاتی که دیوارهای‌آتش فعلی عملاً نمی‌توانند انجام دهند) و جلوگیری از رسیدن این بسته‌ها به مقصد و در نتیجه سد کردن تلاش‌های نفوذی طراحی شده‌اند. چنین قابلیتی بسیار فراتر از قابلیت‌های معمول در IDS ها است که تنها می‌توانند بعد از رسیدن ترافیک خطرناک به قربانی اعلام هشدار کنند یا سعی در جلوگیری از ادامه نفوذ نمایند. IPSها در واقع قابلیت‌های دیوار آتش و IDS ها را با یکدیگر درآمیخته‌اند یک IPS شبیه یک دیوار آتش به طور سری روی خط انتقال قرار می‌گیرد به طوری‌که تمام بسته‌ها باید از داخل آن عبور کنند. بنابراین همین که یک بسته مشکوک تشخیص داده شد و قبل از اینکه به رابط

---

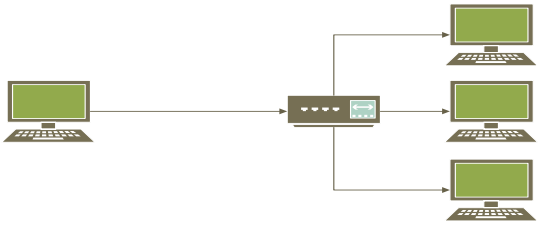
1 . NIDS

2. Intrusion Protect Systems(IPS)

داخلی و شبکه محافظت شده منتقل شود می‌تواند حذف شود. همچنین نشست مربوط به آن بسته می‌تواند به نوعی با عنوان مشکوک علامت‌گذاری شده و در نتیجه تمام بسته‌های مربوط به آن نشست نیز می‌تواند با پردازش کوچکی حذف شود.

به دلیل قیمت مناسب و کارایی قابل قبول، بخش عظیمی از شبکه‌ها با استفاده از هاب، پیاده‌سازی شده‌اند. در شبکه‌ی مبتنی بر هاب، فریمی که هر ایستگاه بر روی کانال قرار می‌دهد توسط هاب دریافت شده و مجدداً بر روی بقیه‌ی کانال‌ها تکرار می‌شود. در یک عبارت ساده‌تر هاب هرچه را دریافت می‌کند به صورت فراگیر بر روی تمام خروجی‌ها ارسال می‌نماید. بنابراین ترافیک تولید شده بر روی یکی از کانال‌های ورودی هاب روی تمام کانال‌های خروجی شنیده خواهد شد. این مفهوم در شکل زیر نشان داده شده است.

شکل ۱) شبکه‌ی محلی پیاده سازی شده با هاب



در چنین ساختاری هرگاه بر روی یکی از ماشین‌های متصل به هاب، یک ابزار اسنیفر نصب شده و فعال باشد، به سادگی قادر به ربودن کل فریم‌های ارسالی از تمام ماشین‌های متصل به هاب خواهد بود. سیاری از نرم‌افزارهای اسنیفر برای محیط‌های مبتنی بر هاب معمولی نوشته شده‌اند. این ابزار به طور عام اسنیفر غیر فعال[1] نامیده می‌شوند و به طور آرام و مخفیانه فریم‌های جاری بر روی شبکه را استراق سمع می‌نمایند.

حمله بر علیه کلمات عبور برای تشخیص هویت

در دنیای شبکه و سیستم‌های رایانه‌ای یکی از روش‌های تأمین امنیت، استفاده از کلمه عبور است. در بسیاری از سازمان‌ها فقط کلمات عبور هستند که از داده‌های محرمانه و حساس حفاظت می‌کنند. بدین معنا که برای هر کاربر یک کلمه عبور در نظر گرفته می‌شود و او باید در هر بار ورود به سیستم (یا شبکه) آن کلمه را وارد نماید. در صورت

[1]. Passive Sniffer

صحت کلمه عبور به او اجازه ورود داده خواهد شد. در حقیقت امنیت مجموعه‌ای از اطلاعات به امنیت یک کلمه عبور، گره خورده است. فاش شدن یک کلمه عبور می‌تواند منجر به از دست رفتن کل اطلاعات کاربر و حتی شکسته شدن حریم کل سیستم شود. لذا امنیت کلمات عبور، از اهمیت بسیار ویژه‌ای برخوردار است. بسیاری از حملات مخرب علیه یک شبکه از طریق کشف کلمات عبور شروع می‌شود. (اسکودیس، ۱۳۸۸: ۹۷)

در اکثر سیستم‌ها برای راحتی کاربران به آن‌ها اجازه داده می‌شود تا شخصاً کلمات عبور مناسب برای خود انتخاب کنند. با این کار امنیت سیستم به عملکرد و سلیقه کاربران وابسته می‌شود و یک کاربر سهل‌انگار می‌تواند امنیت دیگران را هم به خطر بیندازد. به طور معمول کاربران حساسیت زیادی نسبت به امنیت سیستم نمی‌دهند چون اکثراً یا ناآگاهند یا آنکه به عملکرد سیستم بیش از اندازه مطمئن هستند و لذا برای راحتی خود از کلمات عبوری استفاده می‌کنند که به خاطر سپردن آن‌ها زیاد سخت نیست: کوتاه است و گاهی با معنی! لذا در بسیاری از مواقع می‌توان با سعی و خطا کلمه عبور یک کاربر را حدس زد. دزدیدن یا حدس زدن کلمه عبور یک کاربر لقمه‌ی بسیار لذیذی برای نفوذگر است چرا که وقتی جای پای او در سیستم به عنوان یک کاربر معتبر باز شد، عملیات بعدی او می‌تواند به آشکار شدن کلمه عبور دیگران و نهایتاً فروپاشی کل شبکه منجر شود.

حدس زدن کلمات عبور به روش‌های سعی و خطا توسط ابزارهای خودکار، فرآیند چندان سختی نیست و یک تازه‌کار هم می‌تواند آن‌ها را بکارگیرد. اکثر این ابزارها رایگانند و به وفور یافت می‌شوند.

حدس زدن کلمات عبور پیش‌فرض سامانه‌ها برای تشخیص هویت

بسیاری از سیستم‌های عامل، سرویس‌دهنده‌ها و حتی سخت‌افزارهایی مثل مسیریاب، دارای یکسری کلمات عبور پیش‌فرض هستند که توسط سازنده آن‌ها تعریف شده است و به خریدار امکان می‌دهد تا وقتی برای اولین بار سیستم را نصب و پیکربندی می‌کند راهی برای ورود به سیستم داشته باشد. این موضوع برای اکثر سیستم‌ها عمومیت دارد. انتظار می‌رود که پس از نصب و پیکربندی، سریعاً کلمات عبور پیش‌فرض با کلمات عبور مشکل و غیرقابل حدس زدن، جایگزین شوند ولیکن مسئولین مشغول و گرفتار (یا بی‌اطلاع و تنبل) حذف یا تغییر کلمات عبور پیش‌فرض را فراموش می‌کنند. یک نفوذگر با آگاهی از کلمات

پیش‌فرض، سعی در امتحان آن‌ها می‌کند و چه بسا بدون هیچ دردسری بتواند با یکی از آن‌ها به سیستم وارد شود.

سیستم‌های شناسایی نفوذ[1]

برای کشف هرگونه تلاش که منجر به فروپاشی یک سرویس دهنده یا پروسه می‌شود به یک سیستم IDS (سیستم تشخیص نفوذ) در شبکه احتیاج می‌باشد. سیستم IDS به طور معمول مکانیزم و ویژگی‌های هر یک از انواع حملات را می‌شناسد. به عنوان مثال سیستم IDS می‌تواند برای آگاهی از شروع حمله بر علیه پشته از دو ویژگی زیر استفاده کند:

هرگاه طول داده‌های ارسالی به یک پورت باز از یک حد مشخص و مجاز طولانی‌تر باشد.

هرگاه درون داده‌های ارسالی بر روی یک پورت خاص، کدهای NOP به وفور وجود داشته باشد در حالی که در انتهای آن کدهای اجرائی یافت شود.

فرار نفوذگر از سیستم تشخیص نفوذ:

به دلیل آنکه حملات به پشته امروزه به شدت رایج شده است، به طور نسبی استفاده از سیستم IDS نیز رواج یافته است. بنابراین طبیعی است که امروز شاهد حملات پیشرفته‌تر از نوع درهم شکستن پشته باشیم که سیستم IDS نتواند شروع یک حمله بر علیه پشته را کشف کند.

یافته‌ها

امروزه ادامه حیات و عملکرد موفقیت‌آمیز سازمان‌ها، بستگی کامل به داده‌ها و اطلاعاتی دارد که در اختیار دارند. تصور ادامه فعالیت سازمان‌های این عصر، بدون اطلاعاتی که بتوانند به آن اتکا کنند غیرممکن است. این ذخیره‌های ارزشمند در بانک‌های اطلاعاتی گوناگونی ذخیره می‌شوند و مثل هر اندوخته گران بهای دیگری نیازمند مراقبت و محافظت دائمی هستند.

گرچه در حال حاضر بانک‌های تجاری با بکارگیری فناوری‌های نوین، دارای سرویس‌های دائمی و شبانه روزی هستند، ولی هر گونه تخلل در روند اجرای کار ادامه کار عادی سازمان

---

[1]. Intrusion Detection Systems

مختل خواهد کرد. در تأمین امنیت بانک‌های اطلاعاتی و اطلاعات ارزشمند آن‌ها مراحل مختلفی باید در نظر گرفته شوند.

۱) جمع‌آوری داده‌ها
۲) ویرایش داده‌ها
(۳) به هنگام نگه‌داشتن داده‌ها
۴) تهیه نسخه‌های پشتیبانی
۵) تدوین برنامه‌های بازیابی جهت بکارگیری در هنگام وقوع حوادث و مشکلات
۶) تهیه گزارشات کنترلی حفاظتی دوره‌ای
۷) حفاظت بانک‌های اطلاعاتی در شبکه‌های کامپیوتری
۸) حفاظت داده‌های حساس در هنگام نقل و انتقال‌های الکترونیکی
۹) تهیه گزارش اعمال تغییرات
۱۰) سیستم مدیریت بانک اطلاعاتی
۱۱) مخاطرات بانک اطلاعاتی

با در نظر گرفتن فرآیند بالا برای پیش‌گیری از حملاتی که نظیر سرریز شدن پشته کنترل اجرا را به دست نفوذگر می‌دهد، اقدامات امنیتی زیر باید در دو سطح مد نظر قرار گیرد:
مقابله در سطح مسئول سیستم و گروه امنیتی سیستم: شامل تنظیمات شبکه، نصب سیستم‌های شناسایی نفوذ، پیکربندی سرویس‌دهنده‌ها و به روز نگهداری آن‌ها.
مقابله در سطح برنامه نویسی: شامل رعایت اصول امنیتی در هنگام پیاده‌سازی یک نرم‌افزار و پیش‌گیری از بجا ماندن اشکال یا شکاف امنیتی قابل نفوذ.
به طور کلی دو عملکرد اصلی (IDS) نظارت و ارزیابی، کشف، واکنش، بر همین اساس هر IDS به طور کلی از دو روش مختلف برای تحلیل استفاده می‌کند:

الف- مقایسه‌ی الگو: در مقایسه‌ی الگو، شبیه به نرم افزار ضد ویروس عمل می‌شود. سیستم شناسایی نفوذ دارای یک پایگاه داده‌ای بزرگ از حملات شناخته شده است و یک امضا یا الگوی حمله از این حملات درست می‌کند. وقتی که داده مشاهده می‌شود، IDS الگوها را در آن، مورد بررسی قرار می‌دهد. یک پایگاه داده‌ای در سیستم شناسایی نفوذ وجود دارد که شامل الگوهای حملات شناخته شده است. پایگاه‌داده‌ای امضا در یک سیستم شناسایی نفوذ شامل صدها حملات شناخته شده است. حملات به صورت‌ها و دسته‌های مختلف ذخیره سازی می‌شوند تا کار مقایسهی الگوها آسان‌تر باشد. گاهی یک حمله که

قبلاً شناسایی نشده است، ظاهر می‌شود، اما چون با همان طبقه‌ی حملات دیگر وفق می‌دهد. ممکن است شناسایی شود. پایگاه داده‌ای امضای سیستم شناسایی نفوذ هم مثل نرم افزار ضد ویروس باید مرتب به روز شود. با این حال، روش‌های حملهی جدید به تعداد ویروس‌های جدید تکرار نمی‌شوند. بنابراین، تعداد موارد به روز رسانی می‌تواند خیلی کمتر باشد.

ب- شناسایی موارد غیرعادی: شناسایی موارد غیرعادی مثل برنامه‌ی پیش‌بینی حمله است که در نرم‌افزار ضدویروس استفاده می‌شود. در شناسایی موارد غیر عادی از الگوریتم برای ایجاد نوعی روند منطقی از آنچه اتفاق می‌افتد، استفاده می‌شود. چون خط دفاعی مقایسه‌ی الگو می‌تواند به وسیله‌ی حملات جدید و ثبت نشده شکسته شود، لذا شناسایی مورد غیر عادی برای تدبیر اندیشی در برابر این مشکل اضافه می‌شود.

مدیریت امنیت صحت بانک‌های اطلاعاتی

در مرحله تشخیص هویت اقدامات زیر قابل انجام می‌باشد:

جدول (۱): متغیرهای در مدیریت امنیت

۱	جلوگیری از هویت	به خاطر ارتباطات کارمندان با خارج از سازمان، بعدها احتمال سوء استفاده از این ارتباطات وجود خواهد داشت. معمولا این تهدید خیلی جدی گرفته نمی‌شود، مگر این که طبیعت ارتباطات افراد در عرصه‌ی سیاسی باشد
۲	استراق سمع اطلاعات	این نوع حمله که در هر زمان و طی ارتباط شبکه هم به وقوع می‌پیوندد مربوط به برخی از اَشکال اطلاعات کاربر می‌باشد که ممکن است توسط دیگر کاربران مشاهده شود که مجاز به دیدن آن اطلاعات نیستند. این مطلب بیشتر به محرمانگی و یا نگهداری از اطلاعات سری مربوط می‌شود.
۳	تغییر قیافه	کاربر وانمود می‌کند که کس دیگری است. اگر فرد تغییر قیافه داده بتواند شخص یا رایانه دور را قانع نماید که فرد دیگری نیست، می‌تواند از تمامی حقوق دسترسی کاربر مورد نظر به شبکه رایانه‌ای استفاده نماید
۴	دست کاری	اگر اطلاعات در موقع ارسال یا ذخیره روی دیسک، قابلیت تغییر را داشته باشد، بیانگر آسیب‌پذیری بالقوه آن است .در این حالت صحت کل زیر سؤال خواهد رفت.
۵	انکار	انکار مربوط به تکذیب یک یا چند نفر از کاربران در استفاده از ارتباطات می‌باشد.
۶	سرکار گذاشتن	حمله‌ی سرکاری متفاوت با حملات دیگر و به طور معمول برنامه‌ریزی شده است این حمله جهت ایجاد مزاحمت در دستیابی به وب انجام می‌شود. در این روش درخواست‌هایی به سرویس اینترنت ارسال می‌گردد که امکان تکمیل آن‌ها وجود نداشته باشد. به این ترتیب سرویس‌دهنده چنان مشغول پاسخ‌گویی به حملات می‌شود که به ناچار باید درخواست‌های برقراری ارتباط یک عده را نادیده بگیرد. در این لحظه مزاحم وارد سامانه می‌شود.
۷	مسیردهی نادرست	اگر ارتباطی که برای شخصی در نظر گرفته شده است، به شخص دیگری تخصیص داده شود، مسیردهی نادرست اتفاق افتاده است.

۸	آنالیز ترافیک	این نوع حمله در مواقعی رخ می‌دهد که ارتباط دو شخص مشاهده و اطلاعات آن ارتباط (از قبیل حضور یا عدم حضور، تناوب، جهت، ترتیب، نوع، مقدار و غیره) فراهم شده باشد.
۹	تهدید نرم افزار	امنیت شبکه توسط نرم‌افزارهای مورد استفاده نیز تهدید می‌شود. یک اصل در علم رایانه وجود دارد که می‌گوید: هیچ برنامه‌ای بدون اشکال نیست. حال وجود اشکال در برنامه‌ای که مسئولیتش حفظ بخشی از امنیت است، اشکال امنیتی خواهد بود.

همانگونه که بیان گردید در تهدید تغییر قیافه، کاربر وانمود می‌کند که کس دیگری است. این مطلب به طور کلی در مسائل تأیید اتفاق می‌افتد. اگر فرد تغییر قیافه داده بتواند شخص یا رایانه دور را قانع نماید که فرد دیگری نیست، می‌تواند از تمامی حقوق دسترسی کاربر مورد نظر به شبکه رایانه‌ای استفاده نماید. وقتی که فرد تغییر قیافه داده، امتیاز ویژهی دسترسی را به دست آورد، ممکن است حملهی او ویران کننده باشد.

جدول ۱۰): آسیب‌پذیری‌های عمومی نسل اول اینترنت و حملات نمونه

سرویس امنیت	آسیب‌پذیری‌ها	حملات نمونه
پروتکل انتقال پستی ساده	عدم تعیین اعتبار آدرس مدیران و منبع	تقلید پیام‌های ایمیل با کذب از مدیران تغییر مسیر غیر مجاز پست طغیان یک سامانه (سد آتش) با پست برای جلوگیری سرویس از منابع گمنام
پروتکل کنترل حمل و نقل پروتکل اتصال به یکدیگر[1]	حمل و نقل فاقد امنیت و فاقد تعیین اعتبار آدرس‌های توافق نامه اتصال به یکدیگر حفاظت مرزی غیر مکفی	بسته‌های به سهولت اخذ شده آدرس‌های کلمات عبور شناسایی مقصد و منبع را افشاء می‌کند. کانال‌های فعال و فعالیت ترافیک را آشکار می‌سازند. فریب آدرس منبع ارتباطی (تغییر چهره پروتکل اتصال به یکدیگر) برای ظاهر شدن همچون یک رایانه محرمانه یا مطمئن، اما پاسخ ندادن به درخواست‌های تأیید هدف- برای سقوط هدف «ناقوس مرگ» ارسال خواص داده‌ها که مرزهای مجاز برای سقوط هدف را افزایش می‌دهند.
برنامه تبادل فایل‌ها[2]	مستعار مجاز با ورود به شبکه مهمان (عموم) مهاجم مجاز دسترسی محدود به امکانات	برنامه انتقال فایل‌های گمنام دسترسی سطح اولیه به منابع سامانه را که می‌تواند برای دسترسی توسعه داده شده اهرم‌بندی شود، ممکن می‌سازد. مهاجم ممکن است در استمرار فعالیت‌های مشروع پروتکل انتقال فایل قطع ایجاد کند.
سرویس‌های وب جهانی (بین‌المللی)	پروتکل انتقال متن رمز شده[3] غیر ایمن روش‌های جستجوگر سایت‌های جهانی روی اینترنت پذیرش محتوای فعال	برنامه اجرایی (جاوا اسکریپت و اکتیو ایکس) می‌تواند برای آغاز تأثیرات شرارت آمیز به کار رود. داده‌های مربوط به سرنخ‌ها Cookie به وسیله فعالیت‌های نظارتی یک سایت دیده بانی بر آن سایت جمع‌آوری گردیده است. «تغییر چهره انسان معمولی» یک مرورگر بازدید کننده را در بررسی بین‌المللی از طریق نرم‌افزار فریبنده معمولی اغوا می‌کند.

حدس زدن کلمات عبور از طریق برنامه نویسی برای تشخیص هویت:

حتی وقتی کلمات عبور پیش‌فرض از سیستم حذف شده باشد باز هم نفوذگر ناامید نخواهد شد. روش بعدی او برای ورود به سیستم آنست که چند خط برنامه نویسی کند. دقت کنید

---

[1]. Transmission Control/ Interconnect Protocole (TCP/IP)
[2]. HTTP
[3]. FTP

که مشخصه کاربری[1] آشکار است و محرمانه تلقی نمی‌شود. (مثلاً root، admin و administrator مشخصه‌های معروف و پرکاربرد هستند) او برنامه‌ای می‌نویسد که به طور مکرر کلمات عبور مختلف را جهت ورود به یک سیستم امتحان نماید. این برنامه یکی از این مشخصه‌های کاربری را در نظر گرفته و کلمات عبور مختلف را امتحان می‌کند. این برنامه همچنین یک فرهنگ لغت غنی در اختیار دارد. برنامه به طور خودکار و سریع یک کلمه عبور حدسی را ارسال کرده و بررسی می‌نماید آیا این حدس درست بوده است یا خیر. در صورت نادرست بودن حدس، کلمه عبور دیگری تولید و آن‌را امتحان می‌نماید. این روند تا پیدا شدن کلمهی عبور و ورود به سیستم ادامه می‌یابد. صدها ابزار مختلف بدین منظور نوشته شده و در اختیار عموم قرار گرفته است.

نکته‌ای که باید در مورد ابزارهای حدس کلمات عبور به آن اشاره کنیم آنست که در اکثر سیستم‌ها هرگاه یک کلمه‌ی عبور اشتباه باشد. به طور عمدی بین پنج تا ده ثانیه، دریافت کلمهی عبور بعدی به تأخیر خواهد افتاد. در این حالت امتحان کلمات عبور مختلف، ممکن است روزها یا ماه‌ها طول بکشد که عملاً ممکن نخواهد بود.

گذشته از تأخیر مصنوعی بین دو تلاش متوالی برای ورود به سیستم، در برخی از سیستم‌ها هرگاه دفعات تلاش ناموفق از تعداد مشخصی تجاوز کند، حساب مربوطه به طور کامل غیرفعال می‌شود. شاید چنین روشی را مناسب تصور کنید و احساس شود بدین نحو هیچ نفوذگری نخواهد توانست با سعی و خطا به سیستم وارد شود ولیکن مشکل دیگری را ایجاد خواهد کرد:

یک نفوذگر می‌تواند بدین نحو تمام حساب‌های کاربری افراد یک شبکه را غیرفعال کند و ورود آن‌ها را به سیستم غیر ممکن سازد. بدین نحو نوع دیگری از حمله بر علیه شبکه شکل می‌گیرد که به آن حمله ممانعت از سرویس می‌گویند. در بخش بعد به آن خواهیم پرداخت.

اگر در شبکه، سیستم شناسایی نفوذ (IDS) نصب شده باشد، هرگاه تلاش‌های یک فرد برای ورود به یک سیستم از تعداد مشخصی تجاوز کرد به سرعت آن‌را گزارش می‌کند.

---

1. User ID

شکستن کلمات عبور به‌روش‌های علمی برای تشخیص هویت

معمولاً حدس کلمات عبور و نفوذ از راه دور به سیستم به روش سعی و خطا احتمال موفقیت کمی دارد چرا که اندکی دقت و هوشمندی مسئول شبکه تمام تلاش‌های نفوذگر را عقیم خواهد گذاشت. برای پیدا کردن کلمات عبور یک سیستم از روش‌های دیگری استفاده می‌شود که اصطلاحاً به شکستن کلمهی عبور مشهور است. مکانیزم شکستن کلمه عبور بر این اصل استوار است که در تمام سیستم‌ها کلمات عبور در جایی ذخیره می‌شوند و همچنین در بسیاری از سیستم‌ها، کلمات عبور روی خط ارسال می‌شوند؛ خواه به طور آشکار و معمولی و خواه به صورت رمز شده و پنهانی.

تأیید هویت بدین نحو انجام می‌شود که پس از ارسال مشخصهی کاربر و کلمهی عبور، سیستم در یک فایل محلی، به دنبال آن‌ها می‌گردد. این فایل محلی که امروزه به صورت رمزنگاری شده ذخیره می‌شود فقط در اختیار مسئول شبکه است و توسط او تنظیم می‌شود. هرگاه نفوذگر این فایل را برباید، تلاش در رمزگشایی آن خواهد کرد و بدین ترتیب تمام کلمات عبور فاش خواهد شد و سیستم در اختیار نفوذگر قرار می‌گیرد زیرا او قادر خواهد بود با هرکدام از کلمات عبور کشف شده به سیستم وارد شود.

عمل شکستن کلمه‌ی عبور منوط به آنست که در ابتدا کلمات عبور رمز شده به نحوی استراق سمع یا ربوده شود. برای شکستن رمز کلمه عبور نیاز نیست که کلید رمز بدست آید چرا که از لحاظ عملی چنین کاری ممکن نخواهد بود. مکانیزم شکستن رمز کلمات عبور به شرح زیر است:

ابتدا یک کلمه عبور به صورت حدسی تولید شده و طبق الگوریتمی مشابه با الگوریتم اصلی رمز می‌شود.

وجود آن در فایل رمز شده بررسی می‌شود.

اگر آن کلمه درون فایل پیدا شد کار تمام است در غیر این صورت یک کلمهی حدسی دیگر تولید، رمز و جستجو می‌شود.

یک ابزار شکنندهی کلمهی عبور حدس‌های اولیه در مورد کلمات عبور را به روش‌های متفاوتی تولید و امتحان می‌کند. حدس‌های اولیه نقش بسیار مهمی در احتمال موفقیت آن ابزار در کشف کلمهی عبور دارند. بعضی از روش‌های تولید و امتحان حدس‌های اولیه عبارتند از:

تهیه یک فرهنگ لغت بسیار غنی از کلمات معنی دار و امتحان تک تک آن‌ها.

جایگشت‌های مختلفی که یک کلمه رمز می‌تواند داشته باشد. بدین منظور برای حدس یک کلمه عبور تمام ترکیبات مختلف آن باید امتحان شود.

روش مختلط که از تلفیق دو روش قبلی بدست آمده و احتمال موفقیت آن بیشتر از هر دو روش می‌باشد. در این روش ابتدا کلمات درون یک فرهنگ لغت امتحان می‌شود. در صورت عدم موفقیت، کلمات فرهنگ لغت با استفاده از جایگشت‌های مختلف امتحان می‌شوند.

به خاطر داشته باشید که لازم نیست ابزارهای شکنندهی کلمهی عبور، بر روی ماشین قربانی بکار گرفته شوند بلکه ابتدا کلمات رمز شده به روش‌های مختلفی (مثل استراق سمع) ربوده می‌شوند. بدین ترتیب عملیات شکستن و کشف آن بر روی ماشین نفوذگر با آسودگی خیال و صرف وقت کافی انجام خواهد شد. ابزارهای شکنندهی کلمهی عبور با پردازنده‌های امروزی قادرند هزاران کلمهی عبور را در هر ثانیه امتحان نمایند. به عنوان مثال کلمات موجود در یک فرهنگ لغت پنجاه هزار کلمه‌ای در کمتر از یک دقیقه امتحان می‌شود.

اشراف اطلاعاتی

حضرت علی(ع) در نامه‌ای به مأمور اطلاعاتی مخفی خود ابوالاسود چنین می‌نویسد: (افرادی مانند تو شایسته خیرخواهی برای مردم و لایق نگهداری امانت الهی هستند و بنابراین از گزارش مطالبی که اتفاق می‌افتد و صلاح امت و مردم در اطلاع پیدا کردن من از آن است دریغ مکن زیرا این کار بر تو واجب است و تو شایسته آن هستی)

قبل از حادثه ۱۱ سپتامبر مسوولین ایالات متحده امریکا معتقد بودند با فناوری‌های پیشرفته و ارتش قوی خود می‌توانند از حملات تروریستی مصون بمانند اما پس از این حادثه پی بردند که چگونه عامل انسانی می‌تواند در زمینه‌های اطلاعاتی از سایر عوامل و ابزارهای اطلاعاتی پیشروتر باشد گرچه فناوری مدرن، جمع‌آوری اطلاعات از طریق رسوخ در ارتباطات الکترونیکی و نقشه‌های ماهواره‌ای را آسان می‌سازد اما کاربرد عوامل انسانی همچنان برای فعالیت هر سازمان اطلاعاتی ضروری است

اشراف اطلاعاتی_به عنوان کار ویژه سازمان‌های اطلاعاتی از اهمیت بسیار زیادی در انجام مأموریت سازمانی برخوردار است و در یک نگاه راهبردی در قالب یک فرایند، قابل ارزیابی است از این رو اگر اشراف اطلاعاتی را یک فرایند در نظر بگیریم روندی را که به واسطه آن

اخبار جمع‌آوری می‌شود، به اطلاعات تبدیل می‌گردد و در اختیار سیاست‌گذاران قرار می‌گیرد.

چرخه اطلاعات فرآیندی پنج مرحله‌ای است که توسط آن، داده‌ای خام به اطلاعات مفید تبدیل می‌شوند که عبارتند از: ۱- برنامه‌ریزی و هدایت ۲- جمع‌آوری ۳- پردازش ۴- تولید ۵- انتشار

این فرآیند حاصل فعالیت‌های اطلاعاتی است و از کلیه تلاش‌هایی که توسط سازمان‌های اطلاعاتی در راستای اهداف و طرح‌های اطلاعاتی و با استفاده از شگردها و ابزارهای اطلاعاتی صورت می‌گیرد. در واقع هدف اصلی این فرآیند درک صحیح و به موقع از اخبار و اطلاعاتی مربوط به موضوعی خاص برای سیاست‌سازان و تصمیم‌گیرندگان و فرماندهان جنگ است و تحقق این مأموریت نیز منوط به جمع‌آوری، پردازش، تجزیه، تحلیل و توزیع دقیق و به موقع اطلاعات است تا بتوان با کمک آن تصمیم‌سازی کرد، پیش‌گیری نمود و با کمک آن با تهدید مقابله نمود و در راستای امنیت‌سازی گام برداشت.

فناوری یک واژه نسبتاً جدید است و شاید جایگزین مناسب و خوبی نباشد که به زبان انگلیسی اضافه شده است. فناوری اطلاعات به مجموعه امکانات سخت افزاری، نرم افزاری، شبکه‌ای و ارتباطی به منظور دستیابی مطلوب به اطلاعات گفته می‌شود. مقام معظم رهبری در فرمایشات خود در جمع کارکنان ساحفاجا می‌فرمایند: «آن چیزی که به من و شما سپرده شده چیز کمی نیست این انقلاب ما، این جمهوری اسلامی ما یک نقطه عطفی در تاریخ بشر است شما در حقیقت در یک محاصره اطلاعاتی هستید باید تلاشتان را چند برابر کنید، مضاعف کنید، هوشمندیتان را به کار بگیرید و ابتکار به خرج دهید»

تاکید مقام معظم رهبری در تدابیر حکیمانه خود به ویژه در فرمایش بالا وظیفه سازمان‌های اطلاعاتی نیروهای مسلح را دو چندان و سنگین نموده و شرایط کنونی را برای ما بسیار حساس ترسیم فرموده‌اند که بایستی با هوشمندی و تلاش زیاد به دنبال ارائه طرح‌های نو و جدیدی باشیم.

از دیرباز اطلاعات نقش مهم و حیاتی در زندگی انسان ایفا کرده است. در همین راستا در طول زمان امکانات ارتباطی متعددی ایجاد شد، تا کار جمع‌آوری، ذخیره و توزیع اطلاعات را به نحو مطلوب‌تری انجام دهد. در عصر حاضر فناوری‌های ارتباطی با کامل کردن فرآیند اطلاع‌رسانی و ارتباطات، توزیع اطلاعات را به قدری آسان ساخته‌اند که افراد در هر کجا که باشند در کم‌ترین زمان ممکن به اطلاعات مورد نیاز خود از اقصی نقاط دنیا دست می‌یابند.

نتیجه آنکه شاهد پدیده‌ای به نام وفور اطلاعات و یا به قولی «انفجار اطلاعات» هستیم. در این میان چنان‌چه جوامع اطلاعاتی در چالش با اطلاعات این چنینی قدرت مقابله صحیح و تجزیه و تحلیل مناسب آن‌ها را نداشته باشند، دچار مشکلات متعددی خواهند شد.

فناوری اطلاعات و ارتباطات با دگرگون کردن شیوه‌های گردآوری، نگهداری و پردازش اطلاعات، همچنین امکانات بی نظیری که در تبادل و نشر اطلاعات به وجود آورده، سازوکارهای نبرد را متحول ساخته است. به این ترتیب، با بدست آوردن اطلاعات وسیع و دقیق از موقعیت و وضعیت نبرد نیروهای خودی و دشمن و در عین حال جلوگیری از دستیابی دشمن به همین اطلاعات، می‌توان سرنوشت نبرد را رقم زد (محمدی، ۱۳۹۰: ۹۷).

ایران اسلامی در شرایطی قرار دارد که تهدیدات امنیتی آن روز به روز در حال افزایش است. دشمن اصلی نظام در جدار مرزهای ایران مستقر شده و مترصد فرصتی است که به اهداف خود دسترسی پیدا کند، رهبران امریکا به راهبرد مشترکی طی ۱۰ سال اخیر تاکید داشته‌اند که محور اصلی آن استحاله از درون و فشار از بیرون و تشویق عناصر گروه‌های سیاسی برای بازگشت هواداران به داخل به عنوان بخشی از این راهبرد است. در چنین شرایطی توجه به وظائف سازمان‌های اطلاعاتی (ساحفاها) بسیار مهم است.

دنیای ارتباطات و تولید اطلاعات به سرعت در حال تغییر بوده و ما امروزه شاهد همگرایی آنان بیش از گذشته با یکدیگر هستیم، به گونه‌ای که داده‌ها و اطلاعات به سرعت و در زمانی غیرقابل تصور به اقصی نقاط جهان منتقل و در دسترس استفاده کنندگان قرار می‌گیرد. بدون شک فناوری اطلاعات و ارتباطات تحولات گسترده‌ای را در تمامی عرصه‌های اجتماعی و اقتصادی بشریت به دنبال داشته و تأثیر آن بر جوامع بشری به گونه‌ای است که جهان امروز به سرعت در حال تبدیل شدن به یک جامعه اطلاعاتی است. صرف نظر از تعاریف متنوع و دامنه وسیع کاربرد فناوری اطلاعات و ارتباطات در بخش‌های مختلف زندگی بشری، دسترسی سریع به اطلاعات و انجام امور بدون در نظر گرفتن فواصل جغرافیایی و فارغ از محدودیت‌های زمانی محوری‌ترین دست‌آورد این فناوری است و می‌توان از ارتباطات مطمئن و در دسترس به صورت کارآمد، به عنوان بخشی از ابزار مؤثر در سازمان‌های اطلاعاتی بهره‌گرفت[1].

1 .ICT (Information, Communication & Technology)

بنابراین بکارگیری مطلوب منابع انسانی در سامانه‌های اطلاعاتی و به ویژه استفاده از شیوه‌های نوین ارتباط با آنان در فضای سایبر و متناسب با فناوری ارتباطات و اطلاعات جایگاه خاص و مهمی داشته و برای اجرای صحیح مأموریت محوله و به خصوص جمع‌آوری سامانه‌های اطلاعاتی، در ارتقای اثربخشی اطلاعاتی سازمان دارای اهمیت بالایی است که تأثیر بکارگیری مطلوب فناوری اطلاعات در فضای سایبر برای برقراری ارتباط با منابع انسانی از جهات مختلف از قبیل سرعت، صرف جویی در وقت، کاهش خطرات و...بسیار حائز اهمیت است.

نتیجه‌گیری

نتیجه تحقیق حاصل از تجزیه و تحلیل کیفی انجام شده و اطلاعات جمع‌آوری شده از اسناد و مدارک مرتبط با موضوع تحقیق و مصاحبه با صاحب‌نظران، به شرح زیر می‌باشد:

محقق در این خصوص به این نتیجه رسیده است که روند رو به رشد توانایی و استفاده از فناوری اطلاعاتی و توسعه تکنولوژیکی و رشد به کارگیری شبکه‌های باز، مانند اینترنت قابلیت‌های بیشتری را فراهم آورده و در عین حال چالش‌های تازه‌ای را به دنبال خواهد داشت و برای جلوگیری از نفوذ از طریق تجهیزات فیزیکی به شبکه‌های رایانه‌ای آجا، اولین نکته‌ای که باید مورد توجه قرار گیرد امنیت فیزیکی آن است. اگر امنیت فیزیکی این تجهیزات تأمین نشود، هیچ‌گونه تدبیر امنیتی دیگری برای آن فایده نخواهد داشت. با دسترسی فیزیکی و با داشتن یک رایانه همراه و یک کابل و مقداری دانش هرکس قادر خواهد بود با استفاده از روش‌های بازیابی رمز عبور، کنترل کامل تجهیزات فیزیکی شبکه مانند سوئیچ و مسیریاب را به دست گیرد.

همچنین به صورت متناوب باید مسیریاب را از نظر سیستم‌عامل و پرونده‌های پیکربندی، به روز کرد. از این طریق اولاً حفره‌های امنیتی که در نسخه‌های جدید پوشانده شده اعمال می‌گردد و ثانیاً کارکرد آن بهبود یافته و سرویس‌های جدید به آن اضافه می‌شود.

مورد دیگری که در بررسی مطالب اشاره شده حاصل شده است مراقبت از محیط‌های رایانه‌ای از طریق توسعه نرم افزارهای کیفی، فایروال‌ها، برنامه‌های ضد ویروس، سیستم مدیریت، رمزنگاری و استفاده از سوئیچ با ساختار سلسله مراتبی به منظور عبور بسته‌ها از چندین لایه جهت اعمال کنترل‌های امنیتی بیشتر بر روی آن‌ها و استفاده از رمز عبور

مناسب جهت جلوگیری از دسترسی بدون مجوز به تجهیزات شبکه‌ای است. اولین قدم برای امنیت رمز عبور، انتخاب رمز عبور خوب و محافظت از آن است.
استقرار سرورها در اتاق شیلد جهت جلوگیری از تأثیر تشعشعات الکترومغناطیسی بر روی آن‌ها و نیز ایجاد کانال ارتباطی امن و استفاده از فیبر نوری بجای کابل مسی جهت برقراری ارتباط بین ایستگاه‌های کاری از دیگر نتایج بدست آمده در رابطه با هدف یکم تحقیق می‌باشد.
محقق در رابطه با هدف دوم به این نتیجه رسیده است که هر گونه چارچوب مفهومی که در آینده برای امنیت تدوین می‌شود بخشی لاینفک از ساختار کلی بوده و از همان آغاز فرآیند طراحی به تهدیدات و آسیب‌پذیری‌های موجود بپردازد و در زمینه استخدام و بکارگیری نیروهای مجرب و آموزش مستمر و تخصصی کارکنان ساحفاجا تلاش‌های قابل ملاحظه‌ای لازم است. تکنیک‌های جمع‌آوری اطلاعات و فریب مرتبط با فضای سایبری و قابلیت‌های آن با سرعت بیشتری در حال تغییر است. یکی از مهم‌ترین اجزایی که از نظر امنیتی باید به خوبی محافظت شود، سیستم‌های عامل هستند با به مخاطره افتادن امنیت سیستم عامل، امنیت تمامی اطلاعات از لحاظ محرمانگی، یکپارچگی و دسترس‌پذیری به خطر خواهد افتاد و شاید نفوذ به هیچ جزء دیگری از سیستم به این اندازه از ریسک را دارا نباشد. و نیز نرم‌افزارهای پایه مجاز در ن. م را مشخص و زیر مجموعه را ملزم به استفاده از آن‌ها نماید.
نتیجه کلی که از تحقیق پیش‌رو به دست می‌آید مؤید این واقعیت است در اقدام‌های مقابله اطلاعاتی با نیروهای فرامنطقه‌ای فرآیند ایمن سازی شبکه‌های اینترنتی و سیستم‌ها باید مستمر باشد زیرا آسیب‌پذیری‌های و تهدیدات جدید پیوسته ایجاد شده یا کشف می‌شوند خاطر نشان می‌کند که نه تنها موارد و تعداد حملات سایبری با رو به افزایش است بلکه آسیب‌پذیری‌هایی هم که مهاجم می‌تواند از آن‌ها استفاده کند پیوسته افزایش می‌یابد. نصب و راه‌انداز یک ابزار امنیت شبکه‌ای نمی‌تواند جایگزین تلاش مستمر برای به هنگام سازی سیستم‌های دفاعی گردد امروزه با گسترش قابلیت‌های فناوری اطلاعات و از طرفی افزایش حجم داده‌ها و نیاز به پردازش سریع اطلاعات، بهره‌برداری از این فناوری را برای نیروهای مسلح ج. ا. ا اجتناب ناپذیر نموده است. بدیهی است که بهره‌برداری محصولات

فناوری اطلاعات در ن. م علی‌رغم فواید سودمند، نیازمند توجه جدی به ملاحظات امنیتی است.

امروزه فناوری اطلاعات که بر شاهرگ حیاتی جریان اطلاعات خیمه زده و پنجه‌های خود را در تمامی ارکان سامانه‌های فرماندهی و کنترل اعم از نرم‌افزارها، سخت‌افزارها، بسترهای ارتباطی فرو برده تا چه اندازه تابع تصمیم‌گیری‌های ماست و چقدر تأثیرپذیر است؟ چه کسی تضمین می‌کند که تجهیزات الکترونیکی و رایانه‌های مجهز به اجزاء هوشمند قابل برنامه‌ریزی به محض بکارگیری، اطلاعات مربوط به موقعیت مکانی شبکهی ما را به نزدیک‌ترین پایگاه دشمن اطلاع ندهد؟

نیروهای آجا به سبب مأموریت و وظایف محوله دارای تنوع تجهیزات و توانمندی‌های زیادی می‌باشند، و ناگزیر باید از فناوری‌های اطلاعات به نحو چشمگیری در انجام مأموریت‌ها و وظایف محوله بهره بگیرند، ساحفاجا نیز که بر اساس قانون یکی از وظایف آن حفظ و حراست از منابع اطلاعاتی آجا می‌باشد باید ضمن بهره‌برداری از این فناوری نقاط آسیب‌پذیر و روش‌های نفوذ به شبکه‌های رایانه‌ای که بخش مهمی از فناوری اطلاعات را تشکیل می‌دهد، به طور کامل شناسایی و با آن‌ها مقابله نماید.

برای حفاظت و حراست و برقراری امنیت اطلاعات و داده‌های با ارزش از طریق تهدیداتی که از جانب تجهیزات ارتباط شبکه و نیز سیستم عامل متوجه آن‌ها می‌باشد باید اصولی را در قالب تکنیک‌ها و روش‌های ذیل رعایت گردد. کلیه تجهیزات باید از لحاظ فیزیکی محافظت شوند و تنها افراد مجاز توانایی دسترسی فیزیکی به آن را داشته باشند.

به طور متناوب باید مسیریاب را از نظر سیستم عامل و پرونده‌های پیکربندی، بروز کرد. از این طریق اولاً حفره‌های امنیتی که در نسخه‌های جدید پوشانده شده را اعمال و کارکرد آن را بهبود بخشیده و سپس سرویس‌های جدید را به آن اضافه کرد.

گزارش‌گیری از وضعیت و کارکرد تجهیزات شبکه، و اطلاع یافتن مدیر شبکه از ضعف‌ها و نحوه‌ی کار آن و دلیل بروز اشکال در آن که این گزارشات شامل دسترسی‌های غیرمجاز به مسیریاب و نیز تغییرات در پیکربندی آن است.

ایجاد آزمایشگاه جهت تست امنیتی تجهیزات ارتباطی شبکه.

بکارگیری به موقع و مفید تجهیزات.

بررسی متناوب عملکرد سیستم و رفع اشکالات آن: این بررسی‌ها به مدیریت این امکان را می‌دهد تا با در نظر گرفتن خطرات امنیتی موجود، ضمن رفع اشکالات شناخته شده سیاست و برنامه امنیتی متناسب و متوازنی را اتخاذ کند.

تهیه نسخه پشتیبان از اطلاعات مسیریابی مسیریاب جهت جایگزینی آن با اطلاعات دست‌کاری شده مسیریاب توسط نفوذگران.

استفاده از سوئیچ‌ها با ساختار سلسله مراتبی

کنترل دسترسی پورت‌های پیکربندی سوئیچ

الف: در حوزه فن آوری اطلاعات

بکارگیری تجهیزات امنیتی مناسب در شبکه شامل مانیتورینگ فعالیت کاربران، فایروال بومی و تأیید شده.

نصب و راه‌اندازی نرم‌افزار تشخیص نفوذ به منظور شناسایی حملات شناخته شده، آنالیز آماری ترافیک غیرنرمال، کنترل و آنالیز فعالیت کاربران و رایانه‌ها، آنالیز ترافیک نرمال، ثبت رویدادها.

تهیه پشتیبان دوره‌ای و منظم از اطلاعات سرویس‌دهنده‌ها و نگهداری آن‌ها در محلی مناسب و در فاصله دور از محل سرویس‌دهنده‌ها.

نصب آخرین وصله‌های امنیتی تولید شده.

نصب و راه اندازی شبکه به روش دامنه جهت اعمال سیاست امنیتی و تعیین میزان دسترسی کاربران به اطلاعات مورد نیاز.

اعمال سیاست‌گذاری مناسب در خصوص شرایط تعیین کلمه عبور کاربران و تعیین زمان‌بندی مناسب جهت تغییر آن‌ها در فواصل زمانی منظم.

مدیریت آدرس‌های IP شبکه.

ب: در حوزه کارکنان

استخدام کارکنان متخصص و متعهد: بازنگری و تغییر سریع با نگاه تحولی به مدیریت گزینش کارکنان با توجه به آسیب‌های گذشته در حوزه استخدام با بهره گیری از گزینش استخدام شایسته محور و اطمینان بخش.

۲) آموزش: برگزاری دوره‌های آموزشی فن‌آوری و امنیت اطلاعات به صورت مستمر برای توسعه دانش و مهارت کارشناسان.

۳) نظارت و کنترل بهینه کارکنان: اعمال نظارت و کنترل مستمر نامحسوس و مؤثر بر رفتار و عملکرد کارکنان که احساس نمایند در هر حال تحت مراقبت و کنترل نامرئی و نامحسوس قرار دارند.

۴) حرفه گرایی در مشاغل: طراحی مطلوب ساختار سازمانی و مشاغل و تدابیری نظیر چرخش شغلی، توسعه شغلی و غنی سازی شغل مدت توقف در شغل در کنار برنامه ریزی مناسب آموزشی و توسعه قابلیت‌ها و شایستگی‌ها و مهارت‌های کارکنان منجر به حرفه گرایی در مشاغل عملیاتی و امنیتی خواهد شد.

منابع:

- احمدپور داریانی، محمد، کارآفرینی، (۱۳۸۷) تعاریف و الگوها، ناشر شرکت پردیس،
- ادوارت والترز، ترجمه غلام علی جان‌گداز، (۱۳۸۶) عملیات و اصول جنگ اطلاعات، تهران، انتشارات دانشکده امام باقر علیه‌السلام.
- اسکودیس، اد، مترجمین ابوالفضل طاهریان ریزی و داوود تاتی بختیاری، (۱۳۸۸) آموزش گام به گام هک و ضد هک، انتشارات سها دانش،
- بیژنی، شهریار، (۱۳۸۳) مقدمه‌ای بر امنیت شبکه داخلی پژوهشکده پردازش هوشمند علائم ، ۳۸-۲۶
- رضائیان، علی(۱۳۷۴) اصول مدیریت، سازمان مطالعه و تدوین کتب علوم انسانی.
- سادوسکای، جورج(۱۳۸۸) راهنمای امنیت فن‌آوری اطلاعات، مترجم‌ین مهدی میردامادی و زهرا شجاعی، دبیرخانه شورای عالی اطلاع رسانی.
- شولسکی، آبرام(۱۳۸۶) نبرد بی‌صدا، ترجمه معاونت پژوهشی دانشکده امام باقر، تهران: انتشارات دانشگاه امام باقر،۱۳۸۱.
- ضیائی پرور، حمید(۱۳۸۶)جنگ نرم ۱ ویژه جنگ رایانه‌ای، موسسه فرهنگی مطالعات و تحقیقات بین‌الملل ابزار معاصر تهران،
- ---------- (۱۳۸۳)جنگ نرم، تهران موسسه فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر.
- علوی‌فر، سید ناصر(۱۳۸۳)جهان زیر سلطه سازمان‌های اطلاعاتی، تهران: نشر دواوی،۱۳۸۲.
- علی احمدی، علیرضا، شمس عراقی، شراگیم(۱۳۸۳) فناوری اطلاعات وکاربردهای آن، انتشارات تولید دانش.
- دولتخواه، سهراب (۱۳۸۸) نقش عوامل انسانی در جمع آوری اطلاعات در عصر ارتباطات؛ فصلنامه امنیت پژوهی شماره ۲۵؛ بهار ۸۸؛ دانشکده علوم فنون فارابی.

- کاب، چی(۱۳۸۳) امنیت شبکه برای همه، ترجمه معاونت پژوهشی دانشکده امام باقر (ع)، انتشارات دانشکده امام باقر (ع).
- کاری لو، جان، (۱۳۸۳)، نفوذگری در شبکه و روش‌های مقابله»، مترجمین عین‌الله جعفرنژاد قمی و ابراهیم عادل محرابی، نشر علوم رایانه، بابل، ۸۶
- کولاتر، نیک(۱۳۸۴)بمباران به سرعت خیال، اطلاعات در عصر آینده جنگ الکترنیکی، نشریه مجموعه مقالات اطلاعاتی، امنیتی، جلد چهارم، تهران: معاونت پژوهشی دانشکده امام باقر (ع)، ۱۱۶
- لشینسکی، آدام (۱۳۹۰)آشنایی با استانداردهای بی سیم، ماهنامه شبکه ترجمه کیومرث سلطانی، شماره ۱۲۶، آذرماه.
- مایک، کلاو (۱۳۸۸) تهاجم و حفاظت سایبری؛ مترجم: عبدالحسین طائفی؛ تهران، انتشارات دانشگاه عالی دفاع ملی؛
- محمدی، مصطفی(۱۳۹۰)فناوری اطلاعات و ارتباطات: جنگ‌های آینده ۲۷، ماهنامه اطلاعات راهبردی شماره ۹۷،
- منصور، جهانگیری(۱۳۷۹) مجموعه قوانین و مقررات نیروهای مسلح،.
- میرسپاسی، ناصر (۱۳۷۹)مدیریت راهبردی منابع انسانی و روابط کار»، تهران: نشر میر.
- نهاوندیان م؛ و حاجی‌زاده ف. (۱۳۷۹)تکنولوژی اطلاعات و اشتغال»، مجلهٔ مصاف (مهندسان صنایع ایران فردا)، ش ۱۹ و ۲۰، ص ۶۳،۶۸
- هیلبزگری، گریس(۱۳۸۱)جنگ پست مدرن، سیاست نوین درگیری، مترجم احمدرضا تقاء تهران: دانشکده فرماندهی و ستاد سپاه،.
- وفایی، محمد(۱۳۸۸)بررسی شیوه‌های نوین جاسوسی؛ فصلنامه جامعه اطلاعاتی، شماره دوم؛ زمستان ۸۸؛ دبیرخانه شورای هماهنگی اطلاعات.
- سادوسکای، جورج، (۲۰۰۵) راهنمای امنیت فن‌آوری اطلاعات، مترجمین مهدی میردامادی و زهرا شجاعی، دبیرخانه شورای عالی
- Hruska Jan, (2009), Computer viruses and Antiviruses Warfare
- Internet Security Policy (A Technical Guide) http://csrc.nist.gov/ispty 2008
- Robert J. Bunker (2005), "Non State Threats and Future Wars", London: Routledge