دانشگاه صنعتی خواجه نصیرالدین طوسی
دانشکده مهندسی صنایع

طرحی جامع برای پیاده سازی و اجرای یک شبکه ملی هانی‌پاتی(هانی‌نت) برای ایران

دانشجو:

مسعود مردان نیا

استاد راهنما: دکتر شهریار محمدی

پایان‌نامه جهت اخذ درجه کارشناسی ارشد

رشته فنآوری اطلاعات گرایش تجارت الکترونیک

شهریور ۱۳۹۱

شکر خدا که هر چه طلب کردم از خدا بر منتهای همت خود کامران شدم

این پایان‌نامه با تمام وجود به تقدیم می‌شود به:

پدر و مادر عزیز ، دلسوز و مهربانم که در هر چه دارم و هر جا که هستم بخاطر وجود مقدسشان است.

دانشگاه صنعتی خواجه نصیرالدین طوسی
دانشکده مهندسی صنایع

طرحی جامع برای پیاده سازی و اجرای یک شبکه ملی هانی‌پاتی(هانی‌نت) برای ایران

مسعود مردان‌نیا

تأیید هیئت داوران:

دکتر شهریار محمدی

استاد راهنمای پروژه

دکتر محمد جعفر تارخ

داور داخلی

دکتر محمود احمدیان عطاری

داور خارجی

پذیرش دانشکده:

دکتر محمد جعفر تارخ

نماینده تحصیلات تکمیلی دانشکده

تأییدیه پایان‌نامه کارشناسی ارشد توسط دانشجو

عنوان پایان‌نامه: **طرحی جامع برای پیاده سازی و اجرای یک شبکه ملی هانی‌پاتی(هانی‌نت) برای ایران**

نام دانشجو: مسعود مردان‌نیا

شماره دانشجویی: ۸۸۰۸۰۷۴

استاد راهنمای پروژه: دکتر شهریار محمدی

اینجانب مسعود مردان‌نیا دانشجوی کارشناسی ارشد رشته مهندسی فناوری اطلاعات گرایش تجارت الکترونیک دانشکده مهندسی صنایع دانشگاه صنعتی خواجه نصیرالدین طوسی گواهی می‌نماید که تحقیقات ارائه شده در پایان‌نامه تحت عنوان فوق الذکر توسط شخص اینجانب انجام شده است و صحت و اصالت مطالب نگارش شده مورد تأیید می‌باشد و در هر جا که از مطالب نگارش شده دیگری استفاده شده است با ذکر منبع و مأخذ می‌باشد. به علاوه گواهی می‌نماید که مطلب مندرج در پایان‌نامه تا کنون برای دریافت هیچ نوع مدرک یا امتیازی توسط اینجانب یا فرد دیگری در هیچ کجا ارائه نشده است و در تدوین متن پایان‌نامه شیوه نگارش مصوب دانشکده مهندسی صنایع را بطور کامل رعایت نموده‌ام. چنانچه در هر زمان خلاف آنچه گواهی نموده‌ام مشاهده گردد خود را از آثار حقیقی و حقوقی ناشی از دریافت مدرک کارشناسی ارشد محروم می‌دانم و هیچگونه ادعایی نخواهم داشت.

نام و نام خانوادگی: مسعود مردان‌نیا

امضا و تاریخ: ۱۳۹۱/۶/۲۰

حق طبع و نشر و مالکیت نتایج

۱- حق چاپ و تکثیر این پایان‌نامه متعلق به نویسنده آن می‌باشد. هرگونه کپی‌برداری بصورت کل پایان-نامه یا بخشی از آن تنها با موافقت نویسنده یا کتابخانه دانشکده صنایع دانشگاه صنعتی خواجه نصیر الدین طوسی مجاز می‌باشد.

۲- کلیه حقوق معنوی این اثر متعلق به دانشگاه صنعتی خواجه نصیرالدین طوسی می‌باشد و بدون اجازه کتبی دانشگاه به شخص ثالث قابل واگذاری نیست.

۳- همچنین استفاده از اطلاعات و نتایج موجود در پایان‌نامه بدون ذکر مراجع مجاز نمی‌باشد.

تقدیر و تشکر

و یزکیهم و یعلمهم الکتاب و الحکمه

به مصداق «من لم یشکر المخلوق لم یشکر الخالق» بسی شایسته می‌دانم از استاد فرهیخته و فرزانه‌ام جناب آقای **دکتر شهریار محمدی** که با کرامتی چون خورشید، سرزمین دل را روشنی بخشیدند و گلشن سرای علم و دانش را با راهنمایی‌های کار ساز و سازنده بارور ساختند، تقدیر و تشکر نمایم.

و همچنین قدردان زحمات کلیه اساتید فرهیخته‌ام در گروه فناوری اطلاعات دانشگاه صنعتی خواجه نصیر طوسی علی الخصوص استاد فرهیخته جناب آقای دکتر محمد جعفر تارخ بوده و همواره از خداوند متعال بهترین‌ها را برایشان خواستارم.

در پایان از کلیه همکاران عزیزم در مرکز فناوری اطلاعات دانشگاه رازی کرمانشاه، علی‌الخصوص مدیریت محترم مرکز جناب آقای دکتر سید وهاب الدین مکی، و کلیه پرسنا توانمند شرکت نوآوران تارنماگستر بخاطر کلیه حمایت‌هایشان سپاسگذارم.

معلما مقامت ز عرش برتر بـــــــاد — همیشه توسن اندیشه ات مظفر بـاد

به نکته های دلاویز و گفته های بلند — صحیفه های سخن از تو علم پرور باد

چکیده

هانی‌پات یکی از جدیدترین فناوری‌ها در زمینه امنیت اطلاعات، و ابزاری مفید برای شناسایی و تحلیل فعالیت-های مخرب بر روی شبکه‌های کامپیوتری است که کارشناسان امنیتی بواسطه آن می‌توانند به یک چارچوب مناسب برای مطالعه و بررسی شیوه‌ها و ابزارهای حمله به شبکه که توسط نفوذگران استفاده می‌شود، دست یابند. به طور یقین حفظ امنیت و پایداری سیستم‌ها و اطلاعات موجود در شبکه ملی اطلاعات کشور و سایر شبکه های بزرگ و کوچک سازمانی امری اجتناب ناپذیر بوده و بکارگیری دانش برقراری امنیت، یکی از مهم-ترین گزینه‌ها برای کاهش این ریسک می‌باشد. راه‌اندازی و استقرار شبکه هانی‌نت یکی از جدید ترین شیوه‌های برقراری امنیت در شبکه‌های کوچک و بزرگ بوده، بطوریکه کشورهای مختلف به دنبال توسعه و محلی نمودن این دانش و بکارگماری آن در شبکه‌های حوزه خود می‌باشند. هانی‌نت مجموعه‌ای از هانی پات‌ها است که در قالب یک شبکه یکپارچه امنیتی، با شناسایی اهداف و رفتار نفوذگر و نقاط ضعف سیستم، در کنار سایر ابزارها، جهت حفظ امنیت شبکه بکار می‌رود. در این پروژه ضمن بررسی روش های مقابله این فن‌آوری با مخاطرات موجود، مدلی جامع برای پیاده سازی یک شبکه هانی‌پاتی در سطح کشور و بهره گیری از ارزش آن برای جامعه امنیتی ارائه می‌شود. انواع هانی‌پات‌ها و قابلیت‌های این راه‌حل‌ها در ابعاد تحقیقاتی و امنیتی بررسی خواهد شد. و در نهایت یک مدل برای استقرار هانی‌پات در زیرساخت شبکه کشور ارائه می‌گردد که می‌تواند گام مؤثری در پیشرفت اهداف امنیتی این شبکه تلقی گردد. پس از ارائه مدل و معماری پیشنهادی خود برای بررسی کارائی سیستم و میزان ترافیک تولیدی در شبکه، با استفاده از روش فرآیندگرا مدل خود را شبیه سازی و بررسی کرده و نتیاج آن در آخرین فصل ارائه می‌گردد.

کلمات کلیدی: *هانی‌پات، هانی‌نت، شبکه ملی اطلاعات، هانی‌پات پویا، امنیت اطلاعات، تشخیص نفوذ، هک*

فهرست مطالب

فهرست جداول نمودارها و اشکال

فصل اول:

کلیات تحقیق

۱-۱ مقدمه

هانی‌پات[1] ابزار مفید و سودمندی برای شناسایی و تحلیل فعالیت‌های مخرب بر روی شبکه است که می‌تواند یک چارچوب برای مطالعه و بررسی شیوه ها و ابزارهای حمله به شبکه که توسط نفوذگران استفاده می‌شود ارائه دهد. این دستاورد یک فن‌آوری نسبتاً جدید می‌باشد که هر روز شاهد افزایش تعداد متخصصان امنیتی علاقه‌مند به این فن‌آوری می‌باشیم و همین امر باعث شده پروژه‌های بسیار متنوعی در سطح ملی و بین المللی برای توسعه این فن‌آوری در جهان تعریف و از سرعت رشد مناسبی برخوردار گردد.

در این فصل ضمن اشاره به مفاهیم اولیه هانی‌پات، مسئله و چالش اصلی مورد نظر این پژوهش مطرح و در ادامه ضرورت انجام این تحقیق و اهداف و دستاوردهای مورد انتظار آن ارائه گردیده است.

۱-۲ بیان مسئله

با توجه به گسترش کاربرد فن‌آوری اطلاعات، مکانیزه کردن اطلاعات و تبادل آن امری اجتناب ناپذیر شده است. به اشتراک گذاشتن اطلاعات و دسترسی به آن‌ها در شبکه‌های عمومی از جمله اینترنت یا شبکه ملی اطلاعات و یا حتی شبکه های شهری و سازمانی با رعایت حقوق دسترسی بسیار معمول گردیده است. بنابراین حفظ امنیت و پایداری سیستم‌ها و اطلاعات آن‌ها از بزرگترین چالش‌های مدیران فن‌آوری و حتی کاربران نهایی می‌باشد. استفاده از تکنولوژی‌های برقراری امنیت شبکه تا حدی می‌تواند این ریسک را کاهش دهد. هانی‌پات یکی از این فن‌آوری‌ها است که می‌تواند با شناسایی اهداف و رفتار نفوذگر و نقاط ضعف سیستم، در کنار سایر تکنولوژی‌های امنیتی جهت حفظ امنیت در شبکه‌ها بکار رود. در این پروژه ضمن بررسی روش های مقابله این تکنولوژی با مخاطرات موجود، مدلی جامع برای پیاده سازی یک شبکه هانی‌پاتی در سطح کشور و بهره‌گیری از ارزش آن برای جامعه امنیتی ارائه می‌شود. انواع هانی‌پات‌ها و قابلیت‌های این راه‌حل‌ها در ابعاد تحقیقاتی و امنیتی بررسی خواهد شد. با توجه به اینکه هانی‌پات به عنوان یک محصول می‌تواند برای پیش‌گیری و تشخیص و یا واکنش به یک حمله عمل کند، در این

1. Honeypot

پایان‌نامه ضمن بررسی مزایا و معایب شبکه هانی‌پاتی ملی نشان خواهیم داد که هانی‌نت[۲] بوسیله جمع آوری اطلاعات در مورد تهدیدات به عنوان یک ابزار تحقیقاتی کاربردی می‌تواند به درک و مقابله بهتر در برابر انواع حملات کمک کند. در این کار تحقیقی، سناریوهای فایروال[۳] و سیستم های تشخیص نفود[۴] متداول را تکرار نخواهیم کرد چرا که همگی این روش‌ها به دلیل حجم داده تولیدی بالا و غیر صحیح، ناکارآمد به حساب می‌آیند. فن‌آوری هانی‌پات برخلاف این سیستم‌ها، بصورت تدافعی عمل نمی‌کند یعنی منتظر پیش‌قدم شدن نفوذگر در شروع حمله نمی‌ماند، بلکه سعی در جمع‌آوری اطلاعات در مورد سبک‌ها و فنون آن‌ها دارد. هانی‌پات برخلاف فایروال که تنها به شناسایی حملات شناخته شده محدود بود، با گردآوری اطلاعات در خصوص حملات صورت گرفته، روش‌های نفوذ جدید را کشف می‌کند[۱].

۱-۳ ضرورت انجام تحقیق

با توجه به گسترش استفاده کاربران از شبکه‌های سازمانی و به ویژه اینترنت، مکانیزه کردن اطلاعات و تبادل آن امری اجتناب‌ناپذیر است. یکی از دغدغه‌های مسئولین کشور نیز جلوگیری از راه‌های نفوذ بیگانگان به شبکه ملی اطلاعات کشور می‌باشد که با هزینه‌های فراوان به مراحل نهایی رسیده و کم‌کم آمادگی لازم را برای ارائه سرویس به هم‌وطنان خواهد داشت. پس حفظ امنیت سیستم‌ها و اطلاعات موجود در این شبکه امری ضروری است. هانی‌پات یکی از این تکنولوژی‌هاست که با شناسایی اهداف و رفتار نفوذگر و نقاط ضعف سیستم، در کنار سایر تکنولوژی‌های امنیتی جهت حفظ امنیت بکار می‌رود.

فن‌آوری هانی‌پات، به نسبت یک تکنولوژی نوظهور بوده که تاکنون از جنبه‌های گوناگون در جهان مورد بحث و پژوهش قرار گرفته است و هر روزه مورد توجه بیشتر متخصصان امنیتی جهان واقع می‌گردد. با توجه به این موضوع که در کشور ما نیز این فن‌آوری مورد توجه مسئولین امنیتی کشور واقع شده و کارشناسان مربوطه به ارزش و لزوم بکارگیری آن برای جلوگیری از نفوذ دشمنان به حریم شبکه ملی اطلاعات کشور و سازمان‌ها پی برده‌اند، پس ضرورت بکارگیری آن در لایه‌های مختلف شبکه کشور امری اجتناب ناپذیر بوده و لزوم انجام این گونه پژوهش‌ها بر متخصصان و مسئولین امنیتی کشور به وضوح مشخص می‌باشد. امید است این پژوهش بتواند گوشه‌ای از این بار پر مسئولیت و وظیفه خطیر را از دوش کارشناسان و متخصصین فعال در این حوزه بردارد.

2. Honeynet
3. Firewall
4. IDS(Intrusion Detection System)

۱-۴ اهداف پژوهش

همان‌طور که می‌دانید یک کامپیوتر قابل حمل مستقل که هرگز به شبکه متصل نمی‌شود و هرگز در هر محیط ناشناخته‌ای در معرض دسترسی قرار نمی‌گیرد، از هر لحاظ دارای ایمنی و اطمینان است. اما با استقرار این سیستم در شبکه‌های کامپیوتری نمی‌توان این‌چنین تصور کرد که هنوز امنیت این سیستم پابرجاست و باید برای امنیت آن چاره‌ای برگزید. سوال این است که آیا ما می‌توانیم به این محیط ها اعتماد کنیم؟ در اوایل، تجارت همیشه رودررو صورت می‌گرفت. در آن زمان در میان مردمانی صورت گرفته که هم‌دیگر را می‌شناختند و در مجاورت هم قرار داشتند. در آن روزها شخص به راحتی می‌توانست معامله را انجام دهد و از صحت آن مطمئن بود.

مشکل مطرح شده توسط محاسبات قابل انتقال[5] بسیار شبیه آن چیزی است که ما در معاملات تجاری در نیمه دوم قرن نوزدهم با آن مواجه بودیم. در طول آن زمان، گسترش نقل و انتقال و شبکه‌های ارتباطی به شکل راه‌آهن و تلگراف، بازارهای تجاری بین المللی را ایجاد کرده بود و مردم مجبور بودند تا کارهای تجاری خود را با افرادی انجام دهند که هرگز آن‌ها را نمی‌شناختند و ملاقات نکرده بودند. بنابراین **اعتماد** نقش مهمی را در تصمیم‌گیری برای قوانین دسترسی به منشاء اطلاعات ایفا می‌کند. مدیریت اعتماد در برگیرنده استفاده از اطلاعات مطمئن که شامل توصیه‌هایی از طرف امانت‌داران می‌باشد. موارد زیر روش‌های مختلف اعتماد می‌باشد[۲]:

- **اعتماد مستقیم:** در مدل اعتماد مستقیم، طرفین هم‌دیگر را می‌شناسند. این مدل شبیه مدل-های اولیه‌ای است که هرکس شخصاً در معاملات تجاری طرف دیگر را می‌شناخت. یک کاربر مطمئن است که یک کلید یا تاییدیه معتبر می‌باشد زیرا او می‌داند که آن متعلق به کجا می‌باشد. (یعنی او را می‌شناسد) امروزه هر سازمانی به این شکل از اعتماد در بعضی راه‌ها از آن استفاده می‌کند. قبل از این‌که آنها انجام معامله‌ایی را شروع کنند باز بینی و بازرسی فیزیکی دقیق انجام شده است. بدنبال آن، آنها معامله را از طریق اینترنت با اعتماد مناسب و با استفاده از تاییدیه‌های قابل اطمینان ومنابع کلید شناخته شده انجام می‌دهند.
- **اعتماد سلسله مراتبی:** در یک سیستم سلسله مراتبی، یک تعداد از تاییدیه‌های بنیانی وجود دارند که بواسطه اعتماد گسترش یافته‌اند. این سیستم شبیه کمپانی مرکزی یک اعتماد را تولید و سپس شرکتهای وابسته از این اعتماد و کلید استفاده می کنند. این تاییدیه‌های بنیانی ممکن است تاییدیه‌های خود را تضمین کنند و یا آنها ممکن است تاییدیه‌هایی را تضمین کنند که همیشه تایید

5. Mobile

کننده تاییدیه‌های دیگری هستند که در پایین سلسله مراتب قرار گرفته‌اند. این مدل از اعتماد توسط CA قراردادی استفاده می‌شود.

- **اعتماد شبکه ای[6] (شبکه‌ایی بواسطه اعتماد)** : این نوع اعتماد شامل مدل‌های قبلی عنوان شده می‌باشد. یک تاییدیه ممکن است بطور مستقیم اعتمادی دانسته شود و یا بصورت بازگشت به تاییدیه بنیانی که بصورت مستقیم قابل اطمینان است مورد اعتماد قرار می گیرند و یا توسط برخی گروه های معرف این کار صورت گیرد. یک اعتماد وبی، از امضاهای دیجیتالی بعنوان معرف استفاده می‌کند. زمانی که هر کاربر کلید دیگری را علامت می‌گذارد (امضاء می‌کند) او معرف آن کلید می-شود. همین‌طور این فرآیند ادامه می‌یابد، که این تعیین کننده یک اعتماد بواسطه شبکه است. PGP[7] نام یک برنامه امنیتی است که از این مدل از اعتماد استفاده می‌کند و روشی برای امضا و رمزگذاری دیجیتالی فایل‌ها و ایمیل‌ها می‌باشد. PGP مفاهیم قراردادی خود از CA استفاده نمیکند. هر کاربر PGP می‌تواند تاییدیه‌های کلید عمومی کاربر دیگر PGP را معتبر سازد. هر چند، این نوع تاییدیه، زمانی برای دیگر کاربران معتبر است که معتبر سازی را قابل اطمینان تشخیص دهد[۲].

این پژوهش بدنبال دستیابی به جدیدترین فن‌آوری‌های مطرح شده در حوزه امنیت اطلاعات علی-الخصوص در حوزه شبکه های رایانه‌ای و طرح آن در حوزه امنیت ملی کشور با اهداف کلی زیر مطرح و اجرا شده است:

- بومی سازی هانی پات در قالب یک هانی نت ملی
- لزوم پیاده سازی و مطالعه دقیق این پروژه در ایران
- متمایز بودن هانی پات ها به نسبت روال های جاری امنیتی از لحاظ نوع دفاع
- پیشنهاد هانی پات‌های مناسب برای شبکه هانی‌نت ملی در سطح کشور جهت توسعه آن

۱-۵ تعریف اصطلاحات

در این پژوهش از ترکیبی از فن‌آوری‌های جدید و قدیمی در حوزه امنیت اطلاعات استفاده شده که در ادامه بصورت خلاصه، اصطلاحات بکار گرفته شده در این نوشتار تعریف شده است:

6. Web of trust
7. Pretty Good Privacy

- هانی‌پات: هانی پات یک ابزار امنیتی است که ارزش آن در کشف و بررسی شدن، مورد حمله قرار گرفتن و به خطر افتادن است[۳]. به عبارتی با به دام انداختن نفوذگر در یک محیط قرنطینه، کلیه فعالیت‌های وی را ضبط کرده و در اختیار کارشناسان امنیتی قرار می‌دهد.

- هانی‌نت: هانی‌نت یک شبکه کاملاً کنترل شده و منفرد از سایر قسمت‌های شبکه ما می‌باشد و معمولاً از چندین هانی پات با سیستم عامل ها و یا چارچوب[۸] های مختلف تشکیل می‌شود[۴].

- فایروال: دیواره آتش[۹] می‌تواند یک دستگاه سخت افزاری و یا یک برنامه نرم افزاری و یا ترکیبی از هردو باشد. یک فایروال خوب می‌تواند جلوی دسترسی نفوذگر به داخل سیستم شما را بگیرد، در ضمن نمی‌گذارد هیچ‌گونه اطلاعاتی بدون اجازه شما از کامپیوترتان خارج شود. فایروال نمی-تواند مستقیماً جلوی حمله ویروس‌ها را بگیرد اما گاهی جلوی ویروس‌ها را برای ارسال ایمیل از یک کامپیوتر آلوده می‌گیرد. بطورکلی این سیستم با تعریف یک سری قوانین در آن می‌تواند جلوی یک سری از حملات شناخته شده را بگیرد و دسترسی به درگاه[۱۰]های کامپیوترهای موجود در شبکه را محدود نماید[۵].

- سیستم های تشخیص نفوذ[۱۱]: سیستم های نرم افزاری یا سخت افزاری هستند که بطور خودکار بر جریان ترافیک شبکه یا یک میزبان منفرد نظارت کرده و ترافیک موجود را بر اساس مشکلات امنیتی و علایم بارز آن مورد آنالیز دقیق قرار می‌دهند. و در نهایت می‌توانند اخطارهای لازم را برای مدیران امنیتی سیستم ارسال نمایند[۶].

- اسنورت[۱۲]: اسنورت یک بسته نرم افزاری متن‌باز[۱۳] است که به منظور پایش ترافیک شبکه به صورت بلادرنگ و نیز آنالیز و لاگ نمودن بسته ها در شبکهIP ، استفاده می‌شود. همچنین قابلیت بررسی براساس الگو و نیز شناسایی حملاتی چون سرریز بافر[۱۴]، حملاتCGI و غیره را داراست[۷]. اسنورت در سه حالت قابل پیکربندی است :

  - شنود کننده بسته[۱۵]: قابلیت مانیتور کردن و نمایش ترافیک شبکه را به مدیر شبکه می دهد. همچنین می‌توان محتویات بسته و نیز محتوی هدر[۱۶] آن را مشاهده کرد .

8. Platform
9. Firewall
10. Port
11. Intrusion Detection Systems (IDS)
12. Snort
13. Open-Source
14. buffer overflow
15. Packet Sniffer

- لاگ کننده بسته[۱۷]: قابلیت شنود بسته را دارد و نیز می‌تواند فعالیت‌های شبکه را در یک فایل ذخیره کند.

- NIDS : در این حالت اسنورت توانایی شناسایی حملات شبکه را داراست. شناسایی این حملات بستگی به قواعدی[۱۸] دارد که در پیکربندی سیستم اسنورت تعریف شده است[۷].

- اکسپلویت[۱۹]: نفوذ بر اساس نتیجه گیری و گرفتن خروجی‌های حاصل از برنامه ها و ابزارها . اغلب موارد نفوذگران و برنامه نویس‌ها هنگامی که سعی به نفوذ به یک کامپیوتر یا یک برنامه را دارند مداوم به آن‌ها داده‌هایی را تحویل می‌دهند که برنامه آن‌ها را پردازش کند و خروجی خود را نمایش دهد در این هنگام نفوذگر با تناسب بستن میان داده‌ها و خروجی‌ها به عملکرد کلی برنامه پی برده و سعی می‌کند که با داده‌هایی که برنامه برای انجام آن‌ها دچار خطا می‌شود به آن‌ها صدمه وارد کند. و از جهتی چون چک کردن برنامه‌های مختلف و کدها وقت زیادی را می‌گیرد فرد نفوذگر وقتی نحوه صدمه زدن به برنامه را کشف کرد برنامه‌ای را برای این منظور می‌نویسد که خودکار کارهای مورد نظر وی را انجام دهد. به همین دلیل هنگامی که یک مشکل امنیتی پیدا می‌شود فرد برنامه نویس کدی را با مضمون اکسپلویت قرار می‌دهد که نقش وی را بهتر و سریع تر انجام دهد[۸].

- دی ام زی[۲۰]: به معنی محوطه محافظت شده می‌باشد. اغلب شرکت‌های ارائه دهنده خدمات اینترنت[۲۱]و یا شرکت‌های بزرگ مصرف کننده اینترنت، سرور هائی دارند که مایل نیستند در شبکه معمولی و داخلی آنها قرار بگیرد و معمولاً نیاز دارند که از خارج از سازمان دیده شوند که دسترسی به این سرورها از اینترنت نیز باید کاملاً تحت کنترل بوده و از این سرورها به سختی محافظت شود[۸].

- شبکه ملی اطلاعات ایران: تا بحال برای این شبکه تعاریف گوناگونی مطرح شده است. اما ما در اینجا به تعریفی که وزیر محترم ارتباطات ایران برای این شبکه مطرح نموده‌اند بسنده می‌نمائیم. شبکه ملی اطلاعات به عنوان یک راه حل اساسی به منظور افزایش امنیت در فضای سایبر، ایجاد خواهد شد. با ایجاد شبکه ملی اطلاعات، شبکه‌های داخلی از اینترنت جدا خواهند شد. بر همین

---

16. header
17. Packet Logger
18. rule
19. Exploit
20. DMZ (Demilitarized Zone)
21. ISP (Internet Service Provider)

اساس در کنار شبکه ملی اطلاعات، اینترنت به منظور استفاده‌های کاربردی عمومی و دریافت اطلاعات مورد نیاز که در شبکه داخلی در دسترس نیست، استفاده خواهد شد. استفاده از اینترنت برای ارسال اطلاعات ارزشمند قابل اتکا نبوده و شبکه ملی اطلاعات به عنوان یک راه حل اساسی در این حوزه پیش بینی شده و اقدام‌های لازم برای افزایش ضریب امنیت روی آن در حال اجرا است. آمادگی دفاعی و حفاظت در برابر خطرات از ابتدای خلقت آدم وجود داشته و با گذشت دوران، پیچیده تر شده است. با توسعه زیرساخت‌های ارتباطی و الکترونیکی شدن امور، تهدیدهای پیچیده‌ای ایجاد شده که نباید از آن ها غافل بود. فن‌آوری اطلاعات یک لایه است و در همه دستگاه‌ها جریان دارد که غفلت از موضوع آسیب‌های احتمالی موجود می‌تواند صدماتی را متوجه مجموعه و کشور کند. مهمترین مشخصه این فضا، نهفته بودن و خاموش بودن آن است و آسیب-های فیزیکی به سرعت قابل شناسایی هستند اما اثرات حملات در فضای سایبری بعد از مدتی مشخص می‌شود. امنیت موضوعی است که همراه هر پدیده و تکنولوژی باید تعریف شود و بحث پدافند غیر عامل نیز در کنار امنیت می بایست مورد توجه قرار گیرد. آنچه در پدافند غیر عامل می‌بایست مورد توجه قرار گیرد، فن‌آوری اطلاعات در بخش های مختلف نظیر فن‌آوری اطلاعات در صنعت است.

- دورکاری[۲۲]: هرگونه شکلی از بکارگیری فن‌آوری‌های اطلاعاتی به جای مسافرت های مربوط به کار و حرکت کار به سمت کارکنان، به جای حرکت کارکنان به سوی کار می‌باشد. دورکاری یک شغل نیست، بلکه یک روش سازماندهی کار است که حول پردازش اطلاعات ساخته می‌شود. افراد یا گروه هایی از افراد، دور از کارفرما، مشتری یا طرف قرارداد، کارشان را انجام می‌دهند: کاری که مستلزم استفاده از انواع گوناگون تجهیزات الکترونیکی است[۹]. در واقع دورکاری نوعی شیوه کار است که به شاغل اجازه می‌دهد بدون نیاز به حضور در اداره تکالیف و وظایف حرفه‌ای خود را به دور از کاغذ بازی های سنتی با انعطاف پذیری بیشتری انجام دهد که یکی از اصول توسعه آن فن‌آوری اطلاعات است. در واقع به واسطه به وجود آمدن کامپیوتر ها، شبکه های ارتباطی، نرم افزارهای ارتباطی و نرم افزارهای اداری و تخصصی علوم مختلف است که امروزه می توانیم از کار از راه دور صحبت کنیم. بطوری که با پیشرفت این ابزارها، تعداد مشاغل از راه دور بیشتر و کارهای از راه دور با کیفیت تر ارائه می‌گردند و نوع جدیدی از کسب و کار در حال شکل‌گیری است[۱۰].

- امنیت[۲۳]: بطور کلی امنیت شبکه رویکردی است که طی آن یک شبکه در مقابل انواع مختلف تهدیدات داخلی و خارجی امن می‌شود، که هر حجم اطلاعات و دانش سازمان بالاتر می‌رود نقش

22. Teleworking
23. Security