ساختار امنیت کاربردی در بهره‌برداری از شبکهٔ اینترنت

حجت‌الله ناصرپور[۱]
حمیدرضا شفاعت[۲]
بهمن دانش‌تبار[۳]

تاریخ دریافت: ۱۳۹۶/۰۱/۱۶ تاریخ پذیرش: ۱۳۹۶/۰۳/۱۱

چکیده

جهان در دهه‌های اخیر شاهد تحولات چشمگیری در حوزه‌های فنّاوری به‌ویژه فنّاوری اطلاعات و ارتباطات بوده است و این تحولات عملاً زندگی فردی و اجتماعی بشر را دگرگون ساخته و وابستگی کلانی را ایجاد نموده است. امروزه دیگر شکی نیست که اطمینان از ایمن‌بودن ساختارهای اطلاعاتی و تجهیزات زیرساخت فنّاوری اطلاعات در سازمان‌ها، کلید فرصت‌های پیش رو، محسوب می‌شوند. موضوع مهم در استفاده از این شبکه، اطمینان‌نداشتن از محیط اینترنت و آسیب‌پذیری و امکان نفوذ و ضربه از طریق عوامل تهدیدکننده در این بستر ارتباطی است. به دلیل اینکه قواعد بازی در شبکهٔ اینترنت توسط کشورهای غالب و پیشرو در علم و فنّاوری اطلاعات و ارتباطات تدوین شده است، ما ناچار باید در این ساختار حضور پیداکرده و ایفای نقش کنیم؛ بنابراین مسئله‌ای که با آن مواجه هستیم، سلامت این حضور و بهره‌برداری از این بستر است. ازاین‌رو پژوهشگران برای پاسخ به این دغدغه تلاش نموده‌اند که به این سؤال پاسخ دهند که «ساختار امنیت کاربردی در بهره‌برداری از شبکهٔ اینترنت کدام است؟» روش پژوهش کمّی و روش‌شناسی پژوهش توصیفی-تحلیلی از نوع پیمایشی بوده است که از ابزار پرسش‌نامه برای جمع‌آوری اطلاعات بهره برده شده است. حجم نمونه ۴۵ نفر تعیین و پرسش‌نامهٔ محقق‌ساخته در میان کارشناسان امنیتی و اطلاعاتی توزیع شده است. از نرم‌افزار اس‌پی‌اس‌اس برای ثبت و تجزیه‌وتحلیل آماری اطلاعات استفاده شده است. یافته‌های پژوهش فرضیهٔ مطرح‌شده را تأیید نموده و نتایج حاکی از آن است که برای مقابله با تهدیدات امنیتی شبکهٔ اینترنت، تلفیقی از اقدامات پیشگیرانه، تدافعی و تهاجمی ضرورت دارد که در قالب ساختار امنیت کاربردی ارائه گردیده است.

کلیدواژه‌ها: *شبکهٔ اینترنت، تهدیدات شبکهٔ اینترنت، ساختار امنیت کاربردی.*

---

۱. دکترای مطالعات امنیت ملی، دانشگاه عالی دفاع ملی (hojat.np90@yahoo.com)
۲. دانشجوی دکترای امنیت ملی؛ دانشگاه عالی دفاع ملی، نویسنده مسئول (hamidrezashafaat@gmail.com)
۳. دانشجوی دکترای امنیت ملی؛ دانشگاه عالی دفاع(mb@gmail.com)

مقدمه

بسیاری از دانشمندان و صاحب‌نظران علوم اجتماعی بر این باورند که ترکیب و هم‌گرایی فنّاوری‌های ارتباطی و تجدید ساختار نظام سرمایه‌داری در دهه‌های اخیر ما را وارد عصر تازه‌ای کرده است. «دانیل بل» آن را «جامعهٔ فرا صنعتی»، «امانوئل کاستلز» جامعهٔ شبکه‌ای و بعضی آن را «جامعهٔ اطلاعاتی» نامیده‌اند. جامعهٔ اطلاعاتی را جامعه‌ای می‌دانند که در آن دسترسی به اطلاعات افزایش‌یافته است و اطلاعات اهمیت زیادی در زندگی روزمره پیدا کرده و سبب تغییراتی در ساختارهای شغلی شده است. به سبب گسترش دامنهٔ تأثیر رسانه‌های جمعی، به‌ویژه ماهواره و اینترنت و سایر فنّاوری‌های اطلاع‌رسانی، جامعهٔ اطلاعاتی امروزه بعدی جهانی پیدا کرد و منحصر به کشور خاصی نمی‌شود (نوابخش و همکاران:۱۳۸۹، ۱۴۷). بیش از دو دهه است که اینترنت نقش بسزایی در ارتباطات جهانی ایفا می‌کند و به‌طور روزافزونی با زندگی مردم جهان عجین شده است. نوآوری‌ها و هزینهٔ کم در این زمینه باعث شده دسترسی، استفاده و عملکرد اینترنت، به میزان توجه‌برانگیزی افزایش یابد، به‌گونه‌ای‌که امروزه اینترنت در سراسر دنیا در حدود ۲ میلیارد کاربر دارد. اینترنت شبکه وسیع جهانی را به وجود آورده که سالانه میلیاردها دلار برای اقتصاد جهانی سودآوری داشته است (خلیلی رکن‌آبادی و علی‌وند، ۱۳۹۱:۱۶۸). باوجوداین، اینترنت دولت‌ها را در مقابل چالش‌های جدید امنیتی قرار داده است. هزینه کم ورود، ناشناس بودن، مشخص نبودن قلمرو جغرافیایی تهدیدکننده، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری و مجازی، موجب شده بازیگران قوی و ضعیف اعم از دولت‌ها، گروه‌های سازمان‌یافته و تارشگری و حتی افراد به این فضا وارد شده و تهدیدهایی همچون جنگ سایبری و مجازی، جرائم سایبری و مجازی، تارشگری سایبری و مجازی، جاسوسی سایبری و مجازی و مانند آن‌ها را به وجود آورند. همین نکته، تهدیدهای سایبری و رایانه‌ای را از تهدیدهای سنتی امنیت ملی که تا حدود زیادی از ماهیت شفافی برخوردارند و بازیگران آن‌ها دولت – ملت‌هایی تشکیل می‌دهند که در یک قلمرو مشخص جغرافیایی شناسایی‌شدنی هستند، متمایز کرده و سبب شده است امنیت ملی به مفهوم سنتی آن در این فضا به چالش کشیده شده و ناکارآمد به‌حساب آید (خلیلی رکن‌آبادی و علی وند، ۱۳۹۱:۱۶۸). امام خامنه‌ای (مدظله‌العالی) دربارهٔ خطر حضور دشمنان در عرصهٔ فنّاوری اطلاعات و ارتباطات فرموده‌اند: «امروز مؤثرترین سلاح بین‌المللی علیه دشمنان و مخالفان، سلاح تبلیغات است؛ سلاح ارتباطات رسانه‌ای است. امروز این قوی‌ترینِ سلاح است و از بمب اتم هم بدتر و خطرناک‌تر است. این سلاح دشمن را شما در بلواهای بعد از انتخابات ندیدید؟ دشمن با

همین سلاح، لحظه‌به‌لحظه، قضایای ما را دنبال می‌کرد و به کسانی که اهل شیطنت بودند، رهنمود می‌داد» (بیانات:۱۳۸۸).

بیان مسئله

تهدیدهای سایبری و رایانه‌ای پدیده‌ای جدید است که در دهه‌های اخیر، هم‌زمان با تحول فنّاوری اطلاعات و گسترش ارتباطات جهانی از طریق شبکه وسیع اینترنت در سراسر جهان ظهور پیداکرده است؛ به‌گونه‌ای که امروزه چالش تهدیدهای سایبری، رایانه‌ای و مجازی، هم مهم و هم پیچیده به نظر می‌رسد. این اهمیت و پیچیدگی ناشی از ماهیت جدید تهدیدهای سایبری و رایانه‌ای و ویژگی‌ها و نمودهای منحصربه‌فردی است که شناخت از آن را بسیار مهم و ضروری می‌نماید (خلیلی رکن‌آبادی و علی‌وند، ۱۳۹۱:۱۶۹). برقراری و حفظ امنیت در فضای مجازی نیازمند تحلیل و بررسی بسیار است. رویدادهای اخیر که خبر آن‌ها از اقصی نقاط جهان به گوش می‌رسد، حاکی از گسترش حملات و ناامنی‌های سایبری در مراکز تجاری، صنعتی و یا حتی دولتی است و بی‌شک نیازمند کسب آگاهی است و برنامه‌ریزی برای مقابله با انواع تهدیدات و حملات را می‌طلبد. ازاین‌رو لازم است برای ورود به این عرصهٔ ارتباطی و اطلاعاتی مجهز وارد شویم تا بتوانیم هم از سرعت سامانه برای تحلیل به‌موقع محیط‌های پیچیدهٔ امنیتی بهره‌برداری کنیم و گام‌های مؤثری برای تولید قدرت ملی برداریم و هم امنیت ارتباط ما در حد اعتمادپذیری برقرار گردد. هرچند نمی‌توان در این محیط با شرایط سرشار از نبود قطعیت، امنیت شبکه را به حد اکمال رسانید. در بررسی پیشینه‌های پژوهش، ساختاری امنیتی کاربردی و مؤثری که بتواند کاربران را در بهره‌برداری از اینترنت به‌طور همه‌جانبه پشتیبانی نماید وجود نداشته و هریک از پژوهش‌های به زوایای متفاوتی از موضوع امنیت بهره‌برداری از شبکهٔ اینترنت اشاره نموده است. با این توصیف پژوهشگران درصدد ارائهٔ ساختاری امنیتی کاربردی بوده که بتواند ابعاد پیشگیرانه، تهاجمی و تدافعی خنثی‌کنندهٔ تهدیدات امنیتی بهره‌برداری از شبکهٔ اینترنت را پوشش دهد.

اهمیت و ضرورت پژوهش

ارتباط و اتصال میان شبکه‌های جهانی را که در اواخر قرن بیستم تکامل یافت و به‌صورت اینترنت نمایان گردید، می‌توان «نظام اعصاب جهانی» برای انتقال اطلاعات حاوی حقایق، افکار و فرصت‌ها «از هر نقطه به نقطهٔ دیگر» توصیف کرد. اینترنت یک ابزار ارتباطاتی با فنّاوری پیشرفته است و میلیون‌ها نفر در سراسر دنیا وارد اینترنت می‌شوند و دنیای وسیعی را به وجود می‌آورند که اصطلاحاً به آن «فضای سایبری و رایانه‌ای» می‌گویند. مرزهای فیزیکی و نیز فاصله جغرافیایی در «دنیای سایبری» تقریباً بی‌معنی است. در اینترنت محدودیت‌های مربوط به

عنصر زمان و مکان معنی ندارد. از این نظر اینترنت یک فضای نسبتاً ایدئالی را برای جاسوسان شبکه‌ای به وجود آورده است. جاسوسی سایبری از رایانه‌ها و دستگاه‌های مربوط به آن استفاده می‌کند تا اطلاعات محرمانه را جمع‌آوری کند. برخلاف جرائم سایبری که مسائل مالی و اقتصادی محرک اصلی مجرمان است، جاسوسی سایبری بیشتر تأثیرات سیاسی داشته و جامعه را تهدید می‌کند. محرک‌های اصلی جاسوسی سایبری متفاوت است؛ اما شامل کسب منافع نظامی، صنعتی، سیاسی و فنی است. جاسوسان سایبری اطلاعات دزدیده‌شده را با اهداف مختلف مورد استفاده قرار می‌دهند که برخی از آن‌ها عبارتند از: تهدید، اخاذی و مختل‌کردن اقدامات رقبای سیاسی(Lord and Sharp, 2011: 17) . گسترش دایرهٔ علوم نظری پیرامون پدیدهٔ نوظهور اینترنت و فضای سایبر، استفاده و بهره‌برداری از ساختاری مناسب و امن از شبکهٔ اینترنت در کشور، بهره‌برداری از اینترنت در راستای افزایش علم و مهارت در جامعه، مقابله با تهدیدات و آسیب‌های مترتب بر استفاده از شبکهٔ اینترنت، به کم‌ترین میزان رسانیدن حملات اینترنتی و ضرورت بهره‌برداری از اینترنت در کسب دانش جدید از اهمیت پرداختن به موضوع است که محققان را بر آن داشته تا به این موضوع بپردازند.

هدف، سؤال و فرضیهٔ پژوهش

هدف اصلی: دست‌یابی به ساختار امنیت کاربردی در بهره‌برداری از شبکهٔ اینترنت

اهداف فرعی:

۱- بررسی تأثیر اقدامات پیشگیرانه در برقراری امنیت شبکهٔ اینترنت

۲- بررسی تأثیر اقدامات تدافعی در برقراری امنیت شبکهٔ اینترنت

۳- بررسی تأثیر اقدامات تهاجمی در برقراری امنیت شبکهٔ اینترنت

سؤال اصلی: ساختار امنیت کاربردی در بهره‌برداری از شبکهٔ اینترنت در کشور چیست؟

سؤال‌های فرعی:

۱- آیا اقدامات پیشگیرانه در کشور در برقراری امنیت شبکهٔ اینترنت مؤثر است؟

۲- آیا اقدامات تدافعی در کشور در برقراری امنیت شبکهٔ اینترنت مؤثر است؟

۳- آیا اقدامات تهاجمی در کشور در برقراری امنیت شبکهٔ اینترنت مؤثر است؟

فرضیهٔ اصلی: ساختار امنیت کاربردی در کشور در بهره‌برداری از شبکهٔ اینترنت با اقدامات پیشگیرانه، تدافعی و تهاجمی شکل می‌گیرد.

فرضیه‌های فرعی:

۱- اقدام پیشگیرانه در کشور در قالب مهارت کاربران، واپایش تجهیزات، رمزنگاری دوره‌ای، نرم‌افزار بومی، سخت‌افزار بومی، سازمان‌دهی و تعادل سامانه و تحلیل محیط و آینده‌پژوهی سایبری در برقراری امنیت شبکهٔ اینترنت مؤثر است.

۲- اقدام تدافعی در کشور در قالب ضدویروس و ضدتروجان، ضدهکر، پایش مستمر شبکه، تلهٔ نظامی، رمزگذاری و شناسهٔ زیست‌شناختی در برقراری امنیت شبکهٔ اینترنت مؤثر است.

۳- اقدام تهاجمی در کشور در قالب هک مراکز حیاتی حریف، طراحی فریب سایبری در برقراری امنیت شبکهٔ اینترنت مؤثر است.

روش پژوهش

این پژوهش مبتنی بر روش پژوهش زمینه‌ای و موردی با استفاده از مطالعهٔ کتابخانه‌ای و اسنادی و فضای اینترنت و همچنین مطالعهٔ میدانی با ابزار سنجش پرسش‌نامهٔ محقق‌ساخته (با پایایی ۸۷٪) است. جامعهٔ آماری خبره به تعداد ۴۵ نفر شامل:۲۰ نفر از دانشجویان مقطع دکترای امنیت ملی دانشگاه عالی دفاع ملی و ۱۰ نفر از کارشناسان فنی و ۱۵ نفر از کارشناسان امنیتی بوده که به دلیل بهرهٔ تخصصی بهتر از دیدگاه افراد جامعهٔ آماری و غنای پژوهش، جامعه تمام‌شماری و به‌عنوان جامعهٔ نمونه تلقی گردیده‌اند. یافته‌های پژوهش با استفاده از نرم‌افزار اس‌پی‌اس‌اس تجزیه‌وتحلیل (توصیفی و استنباطی) گردیده و فرضیه‌های پژوهشی اثبات شده است.

پیشینهٔ پژوهش

با بررسی‌های انجام‌شده در منابع مختلف، فعالیت پژوهشی که عیناً مشابه عنوان یادشده بوده باشد، یافت نگردید؛ اما مقالات مرتبط با متغیرهای موضوع که حاکی از اهتمام به اثربخشی برخی راهکارهای امنیت در شبکهٔ اینترنتی است، دسترس‌پذیر است. در این زمینه می‌توان به موارد زیر اشاره نمود:

۱- خلیلی پور رکن‌آبادی، علی و نورعلی‌وند، یاسر در سال ۱۳۹۱ در پژوهشی با عنوان تهدیدات سایبری و تأثیر آن بر امنیت ملی بیان کرده است که یکی از مهم‌ترین منابع قدرت در هزارهٔ سوم هستند. ویژگی‌های فضای سایبری همچون قیمت پایین ورود، گمنامی، آسیب‌پذیری و ناهم‌تراز بودن، پدیدهٔ انتشار قدرت را به وجود آورده است. بدین معنی که اگر تاکنون دولت‌ها بازی قدرت را تنها میان خود تقسیم کرده بودند، ازاین‌پس باید آن را با بازیگران دیگری همچون شرکت‌های خصوصی، گروه‌های سازمان‌یافتهٔ تارشگری و جنایی و افراد تقسیم نمایند. اگرچه هنوز این دولت‌ها هستند که در این عرصه نقش مهمی را

بـازی مـی‌کننـد. بـالطبع، این پدیده، امنیت ملی دولـت‌هـا را از تأثیرگـذاری خـود بـی‌نصـیب نخواهد گذاشت.

۲- پالیزبان، محسن در سال ۱۳۹۴ در پژوهشی با عنوان بررسی رابطهٔ اینترنـت و امنیـت ملـی جمهوری اسلامی ایران، بیان کرده است که امنیت ملی کشور با اینترنت و امنیت فضای مجازی پیوستگی مثبتی دارد. چگونگی این پیوستگی در حوزهٔ امنیتـی، سیاسـی، فرهنگـی و نظـامی-دفاعی بررسی و ارزیابی گردیده است.

۳- بجانی، صادق؛ حسنی ،آهنگر و محمدرضا، اخضمی مصطفی، در سال ۱۳۹۲ در پژوهشی بـا عنوان نقش سامانه‌های تشخیص نفوذ در امنیت سرویس‌های وب بیان کرده‌اند که سرویس‌های وب، مؤلفه‌های نرم‌افزاری مبتنی بر شبکه‌ای هستند که استفاده می‌کنند و وابسته به هیچ الگـو یا زبان برنامه‌نویسی خاصی نیستند. ویژگی خود توصـیفگری در ایـن کاربردهـا امکـان ترکیـب سرویس‌های مختلف برای ایجاد کاربردهای توزیع‌شده را ممکـن مـی‌سـازد. سـرویس‌هـای وب به‌عنوان یک پیاده‌سازی از معماری سرویس‌گرا، نه‌تنها در اینترنت؛ بلکـه در ارتبـاط‌هـای میـان سازمان‌ها در مهروموم‌های اخیر بسیار مورد توجه قرارگرفته‌اند. از سـوی دیگـر، قرارگـرفتن در معرض حملات بدخواهانه و نفوذگران، قابلیت اطمینـان ایجـاد راهکارهـایی بـرای حفـظ بقـای چنـین سـامانه‌هـایـی در مقابـل حمـلات و نفـوذگران و رعایـت مباحـث پدافنـد غیرعامـل در سرویس‌های وب از اهمیت زیادی برخوردار است. امروزه سامانه‌های تشخیص و پیشگیری نفـوذ برای تکمیل سطوح دفاعی سـازمان‌هـا در فضـای سـایبر، کـاملاً شـناخته شـده هسـتند. ولـی متأسفانه، چنین سامانه‌هایی برای تحلیل وقایع سرویس‌های وب کارایی لازم را ندارنـد؛ چراکـه سرویس‌های وب در سطحی بالاتر از حد تشخیص این سامانه‌ها فعـال هسـتند. کارهـای بسـیار محدودی را می‌توان یافت که به چنین راه حلی دربارهٔ سرویس‌های وب اشاره کـرده باشـند. در این مقاله، راهکاری مناسب برای توسعهٔ سامانه‌های تشخیص نفـوذ در سـرویس‌هـای وب ارائـه گردید. راهکار یادشده، حاصل بررسی وب‌سرویس‌ها، روش‌های تشخیص نفـوذ و سـه معمـاری نظام تشخیص نفوذ در این زمینه است. راهکار پیشنهادی، حاصـل ادغـام روش هـای تشـخیص نفوذ مبتنی بر امضا و مبتنی بر ناهنجاری در سرویس‌های وب است. هـم‌چنـین بـا اسـتفاده از فرایند پاسخ‌دهی و آموزش نظام تشخیص نفوذ، می‌توان کارایی نظام در برابر حملات ناشـناخته را افزایش و میزان هشدارهای غلط در نظام تشخیص نفوذ را کاهش داد.

۴- دهقان شاد، حوری در سال ۱۳۹۰ در پژوهشی با عنوان چگونگی گردش شایعات سیاسی در فضای اینترنت بیان کرده است که مردم شایعه‌هایی را که از طریـق رایانامـه پخـش مـی‌شـود،

بیشتر قبول می‌کنند. شکل بیمارگونه این دایرهٔ باطل آنجاست که ما شایعه‌هایی را که از دوستانمان از طریق رایانامه می‌گیریم، به آشنایان دیگرمان می‌دهیم و این روند همین‌طور ادامه پیدا می‌کند. تمام این جریاناتی که شرح داده شد، موجب بقای شایعه در فضای مجازی می‌شود. باوجود اینکه بیشتر شواهد نشان می‌دهد که این خبرها واقعیت ندارند. البته پژوهشگر در این پژوهش، در مورد تأثیر فیس بوک و توییتر بررسی انجام نداده، گرچه او متذکر شده که این شبکه‌های اجتماعی نیز چون بیشترین تمرکزشان بر حلقهٔ دوستان و آشنایان است، روشن است که مانند رایانامه عمل می‌کنند. پژوهشگر در پایان پژوهش خود گفته است برای کسانی که نگران تأثیرگذاری شایعات انتخاباتی از طریق اینترنت هستند، می‌توان گفت که این تأثیر بسیار نامعلوم است؛ زیرا میزان این تأثیر بر روی هر انسان به دلیل تفاوت‌هایی که مخاطبان با یکدیگر دارند، فرق دارد و ما نمی‌توانیم دقیقاً بسنجیم که به چه میزان مخاطبان سیاسی حاضرند با چشم‌بسته هر آنچه را می‌بینند، بپذیرند. ولی بااین‌حال باید خوش‌بین بود؛ زیرا اوضاع از این هم می‌توانست بدتر باشد. بااینکه تأثیر رایانامه در پخش شایعه نگران کننده است؛ اما به‌اندازهٔ رایانامه‌های شایعه‌پراکن، رایانامه‌های مخالف این شایعات هم در فضای مجازی در حال گردش هستند.

۵- مهدی فهیمی در پژوهشی در سال ۱۳۸۰ با عنوان امنیت اطلاعات و تجارت الکترونیکی بیان کرده است که لازم است سازمان‌ها سه شرط زیر را در طراحی نظام امنیت اطلاعاتی خود مدنظر داشته باشند: الف) اطمینان از سلامت اطلاعات چه در زمان ذخیره و چه هنگام بازیابی و ایجاد امکان برای افرادی که مجاز به استفاده از اطلاعات هستند. ب) دقت: اطلاعات چه از نظر منبع ارسالی و چه در هنگام ارسال و بازخوانی آن باید از دقت و درستی برخوردار باشد و ایجاد امکاناتی برای افزایش این دقت ضرورت خواهد داشت. ج) قابلیت دسترسی: اطلاعات برای افرادی که مجاز به استفاده از آن هستند، باید در دسترس بوده و امکان استفاده در موقع لزوم برای این افراد مقدور باشد.

مفاهیم و مبانی نظری پژوهش

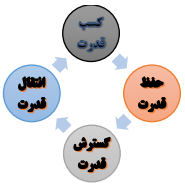
شبکهٔ اینترنت: اینترنت شرایطی را به وجود آورده که در آن، قدرت واپایش بر اطلاعات به میزان بسیار بیشتری توزیع شده است. اینترنت زمینهٔ ارتباطات نامحدود فردبه‌فرد (از طریق رایانامه)، فرد به تعداد بیشتری از افراد را (از طریق تالارهای گفت‌وگوی شخصی یا همایش‌های الکترونیکی) فراهم می‌کند. کارکردهای مثبت اینترنت عبارتند از: اطلاع‌رسانی به سریع‌ترین، گسترده‌ترین و کاراترین شکل؛ افزایش کیفیت و کمیت پژوهش‌های علمی در نشریات بین‌المللی؛ نزدیک‌کردن مردم به هم؛ برقراری ارتباط صوتی و تصویری با اقتصادی‌ترین

روش با دوستان یا همکاران، صرفه‌جویی در وقت و هزینه، از طریق تجارت اینترنتی، امکان دسترسی به عمیق‌ترین و جدیدترین مباحث علمی روز و دانشگاه‌های جهان (کبیری‌فر و صرافی‌زاده، ۱۳۸۹: ۵۹). اینترنت، هم‌چنین قادر است زمینهٔ ارتباط با شمار زیادی از افراد با یک فرد (از طریق پخش نامهٔ الکترونیکی) را فراهم کند. شاید مهم‌تر از این، اینترنت شمار بیشتری از افراد را با شمار بسیاری دیگر (از طریق اتاق گفت‌وگوی هم‌زمان) مرتبط می‌کند. پیام‌های اینترنتی از این توان برخوردارند که به میزان بیشتر و سریع‌تر و با دخالت کمتری از سوی دیگران، جریان پیدا کنند. در این شرایط، حکومت‌ها اگر بخواهند جریان اطلاعات را از راه واپایش اینترنت واپایش نمایند، ناچار به تحمیل هزینه‌های بالایی خواهند شد و در آخر کار از تلاش‌های خود ثمر چندانی نخواهند گرفت. این تحول بدین معنیست که سیاست خارجی، عرصه‌ای نخواهد بود که صرفاً حکومت‌ها در آن حضور داشته باشند؛ بلکه سازمان‌های مرتبط با افراد و بخش خصوصی، در داخل و خارج از کشور از این توان برخوردار خواهند شد که نقش مستقیمی در سیاست جهانی ایفا کنند (نای، ۱۳۸۷ :۱۴۱). درنتیجه، اینترنت از طریق همین ابزارهای ارتباطی، ناراضیان را یک‌صدا کرده تا شنیده شوند و به عموم مردم وسیله‌ای داده است تا سازمان‌دهی شوند. درحالی‌که برخی تحلیلگران نقش اینترنت در انقلاب‌های غرب آسیا و شمال آفریقا را انکار می‌کنند، شبکه‌های اجتماعی همچون توئیتر و فیس‌بوک، نقش بسزایی در شکل‌گیری این حوادث داشته‌اند. از سوی دیگر، اینترنت می‌تواند مورد سوءاستفاده دیکتاتورها و تارشگران نیز قرار بگیرد. به‌عبارت‌دیگر، دیکتاتورها و گروه‌های افراطی نیز با استفاده از همین روش، ایدئولوژی خود را گسترش داده و در سرتاسر دنیا عضو می‌گیرند (شارپ و دیگران، ۲۰۱۱ :۱۴).

اینترنت و قدرت: قدرت به معنای توانایی تأثیر بر افراد دیگر برای دستیابی به نتایج مورد نظر است؛ اما باید توجه داشت، اظهارنظر دربارهٔ قدرت، همیشه به زمینه بستگی دارد و شبکهٔ اینترنت یک حوزهٔ جدید و مهم از قدرت است. ... کشورهایی مانند آمریکا -که منابع عظیمی از قدرت سخت و نرم در اختیاردارند- خود را در حال تقسیم عرصه با بازیگران جدید و مواجه‌شدن با مشکلات بیشتر در واپایش مرزهایشان در حوزهٔ سایبر می‌بینند. اگرچه شبکهٔ اینترنت یا فضای سایبری جای فضای جغرافیایی را نخواهد گرفت و حاکمیت دولت را منسوخ نخواهد کرد؛ اما بی‌تردید شاهد پراکندگی قدرت در فضای سایبر خواهیم بود و همین اعمال قدرت در هر یک از این ابعاد را به‌شدت پیچیده خواهد کرد. همان‌گونه که قدرت[1] موضوع و

1. Power

مبنای جغرافیای سیاسی است و تمامی برداشت‌ها، رویکردها، مصادیق و مؤلفه‌های جغرافیای سیاسی حول مدار و محور قدرت می‌چرخند و عنصر قدرت، به‌صورت نهان و آشکار، خود را در جغرافیای سیاسی نشان می‌دهد و جغرافیای سیاسی بدون قدرت مفهوم و معنایی ندارد (حافظ نیا، ۱۳۷۶ :۱)؛ ازجمله مهم‌ترین عوامل، عناصر و ابزارهای قدرت‌ساز در حوزهٔ فنّاوری اطلاعات و ارتباط می‌توان از اینترنت، مطبوعات، ماهواره‌ها، خبرگزاری‌ها و ... نام برد. اهمیت این ابزارها و عوامل و نیز ارزش و آثار عمیق عملکردی آن‌ها بر تحولات جوامع انسانی تا حدی است که از آن غفلت نورزیده‌اند و از آن به انقلاب تعبیر کرده‌اند[1]؛ یعنی یک تغییر و تحول ریشه‌ای و سریع انتقالی (محسنی، ۱۳۸۰ :۳۷). در جغرافیای سیاسی اطلاعات و ارتباطات نیز موضوع کلیدی برتری اطلاعاتی[2]، تبادل اطلاعاتی[3]، مزیت اطلاعاتی[4]، تمایز اطلاعاتی[5] و در یک‌کلام قدرت است. امروزه دیگر مقاومت در برابر توسعهٔ دیجیتالی ممکن نیست و در این حرکت روبه‌جلو، تنها جوامعی می‌توانند استقلال خود را حفظ کنند که حضوری قدرتمند داشته باشند و هنگامی‌که بحث قدرت پیش می‌آید، از فرایندی به‌نام چرخهٔ قدرت نیز باید نام برد. این چرخه شامل چهار گام است: گام اول در چرخهٔ قدرت در یک نظام اطلاعاتی و ارتباطی، کسب قدرت است؛ یعنی تلاش هماهنگ و هدفمند برای دست‌یابی به قابلیت‌ها، ظرفیت‌ها، توانمندی‌ها و منابع اطلاعاتی و ارتباطی که قدرت‌زا و قدرت افزا باشند. در گام دوم؛ حفظ قدرت مد نظر است؛ یعنی مجموعهٔ اقداماتی که برای تثبیت و تحکیم منابع تولیدکنندهٔ قدرت اطلاعاتی و ارتباطی صورت می‌گیرد و در گام سوم؛ قدرت از طریق تقویت و توسعهٔ عوامل، عناصر و مؤلفه‌های ایجادکننده‌اش، گسترش و توسعه می‌یابد. در گام چهارم؛ قدرت بنا به دلایل و صور مختلف (به‌صورت اختیاری، اجباری، خواسته، ناخواسته و ...) ممکن است به گروه، سازمان یا واحد سیاسی دیگر منتقل شود (شاه‌محمدی، ۱۳۹۰: ۱۳).



شکل شماره ۱- چرخه قدرت (شاه‌محمدی، ۱۳۹۰: 13)

1. Revolution
2. Information Superiority
3. Information Dominance
4. Information Advantage
5. Information Differential

تهدیدات و حملات در شبکهٔ اینترنت: بـه‌مـوازات افـزایش ابعـاد خـدمات‌رسـانی اینترنـت در حوزه‌های مختلف زندگی بشر و بـه‌ویـژه در امور تجاری و بازرگانی، مهاجمان رایانه‌ای، سـارقان و جاسوسان اطلاعاتی، حجـم تهدیـدها و آسیب‌های ناشی از این فنّـاوری را بـه‌شـدت افـزایش داده‌اند. این تهدیدها امروزه افزون‌براینکـه روزبه‌روز گسترش می‌یابند و پیچیـده‌تـر مـی‌شـوند، امنیت ملی کشـورها و دولـت‌هـا را بـه‌طـور مستقیم تحت تـأثیر قـرار مـی‌دهنـد (میرمحمـدی، ۱۳۸۷:۳۶).

تهدیدات و حملات علیه امنیت شبکه: تهدیدات و حملات علیـه امنیـت شـبکه از جنبـه‌هـای مختلف بررسی‌شدنی هستند. از یـک دیـدگاه حمـلات بـه دودسـتهٔ فعـال و غیرفعـال تقسـیم می‌شوند و از دیدگاه دیگر، مخرب و غیر مخرب؛ اما به‌طورکلی می‌توان بر اساس عامل زیر ایـن حملات را تقسیم‌بندی نمود:

حملات متعارف شبکهٔ اینترنت:

حملهٔ قطع سرویس[1]: هدف همهٔ حمله‌ها یک‌چیز است؛ قطع ارتباط رایانه از شبکه در این نـوع حمله، کاربر دیگر نمی‌تواند از منابع و اطلاعات و ارتباطات استفاده کند. این حمله از نوع فعـال است و می‌تواند توسط کاربر داخلی و یا خارجی صورت گیرد.

شنود[2]: در این نوع حمله، مهاجم بدون اطلاع دوطرف تبادل داده، اطلاعات و پیـام‌هـا را شـنود می‌کند. این حمله غیرفعال است و می‌تواند توسط کاربر داخلی و یا خارجی صورت گیرد.

تحلیل ترافیک[3]: در این نوع حمله، مهاجم بر اساس یک‌سـری بسـته‌هـای اطلاعـاتی ترافیـک شبکه را تحلیل کرده و اطلاعات ارزشمندی را کسب می‌کند. این حمله یک نوع حملهٔ غیرفعال است و بیشتر توسط کاربران خارجی صورت می‌گیرد.

دست‌کاری پیام‌ها و داده‌ها[4]: این حمله یک حملهٔ فعـال اسـت کـه در آن مهـاجم جامعیـت و درستی اطلاعات را با تغییرات غیرمجاز به هم می‌زند و معمـولاً توسـط کـاربر خـارجی صـورت می‌گیرد.

جعل هویت[5]: یک نوع حملهٔ فعال است که در آن مهاجم هویت یک فرد مجـاز شـبکه را جعـل می‌کند و توسط کاربران خارجی صورت می‌گیرد. (www.maghaleh.net)

1. Denial – of – Service(DOS)
2. Eavesdropping
3. Traffic analysis
4. Messages and data manipulation
5. Impersonation

حملات و تهدیدات تخصصی شبکهٔ اینترنت:

درِ پشتی[1]: در پشتی، به هر معبر باز در نرم‌افزار، به‌گونه‌ای‌که کسی بتواند بدون اطلاع صاحب و کاربر نرم‌افزار، از آن عبور کرده و به داخل سامانه نفوذ کند، در پشتی گفته می‌شود. در پشتی‌ها بیشتر به دلیل بی‌توجهی ایجادکنندهٔ نرم‌افزار، به‌صورت باز رها می‌شود و همین امر باعث می‌شود افزون‌بر ایجادکننده، دیگران نیز از آن سوءاستفاده کنند.

حقه[2]: فنی است برای دسترسی غیرمجاز به رایانه‌ها، هکر با دسترسی به آی پی یک رایانه شروع به ارسال اطلاعات به سامانهٔ قربانی کرده و خود را مورد اعتماد وانمود می‌کند. (خود را به‌جای یک رایانه مورد اعتماد جا می‌زند).

انسان در میانه[3]: نفوذگر بین دو رایانه که در حال تبادل اطلاعات هستند، قرار می‌گیرد. نفوذگر ترتیبی را اتخاذ می‌کند که دو رایانه از وجود او بی‌اطلاع باشند. سامانه‌های بی‌سیم در معرض این حمله قرار دارند.

بازپخش: وقتی یک هکر به‌وسیله ابزار اسنیفر[4] بسته‌های اطلاعاتی را از روی سیم برمی‌دارد، یک حملهٔ بازپخش رخ داده است. وقتی بسته‌ها دزدیده شدند، هکر اطلاعات مهم و نام‌های کاربری و کلمات عبور را از درون آن استخراج می‌کند.

آی پی/تی سی پی ربایی[5]: معمولاً به آن جعل نشست[6] نیز گفته می‌شود. هکر می‌تواند نشست تی سی پی بین دو رایانه را به دست آورد. یک روش مشهور، استفاده از «منبع تار و مار»[7] کردن آی پی‌هاست؛ یعنی بسته‌های آی پی را طوری تغییر دهیم که از مسیری خاص بگذرند.

مسمومیت دیان اس[8]: این حمله هنگامی است که پوشهٔ دیان اس[9] شما با اطلاعات ناجوری پر شود. به‌صورت ساده‌تر هنگامی است که نفوذگر رکوردهای دیان اس را که به هاست‌های[10] درستی اشاره دارند، به هاست مورد نظر خود تغییر می‌دهد.

نیروی بی‌رحم[11]: یک روش برای شکستن کلمات رمز و به دست آوردن آن‌هاست. حملهٔ بی‌رحم» حروف را به‌صورت ترکیبی استفاده می‌کند و با آزمون کردن آن‌ها، رمز عبور را پیدا

1. back door
2. Spoofing
3. Man in the Middel
4. Sniffer
5. TCP/IP Hijacking
6. Session Hijacking
7. Source-rout
8. Domain Name System poisoning
9. Domain Name System
10. Host
11. Brute force

می‌کند. برای مقابله با این روش باید کلمات رمز با طول زیاد انتخاب کرد و یا کلمات رمز را هر دفعه تغییر داد.

فرهنگ لغت[1]: یک روش برای به دست آوردن کلمات رمز عبور است. کلمه «دیکشنری»[2] در اصل لغت‌نامه‌ای از کلمات معروف است که در یک پوشه ذخیره شده‌اند و به‌وسیلهٔ یک ابزار برای شکستن کلمات رمز، مورد استفاده قرار می‌گیرند. برای مقابله با این حمله باید از کلماتی استفاده کرد که در لغت‌نامه وجود ندارد.

خرناس (شنود): با استفاده از شنود، جذب کلیهٔ اطلاعات شبکه انجام می‌گیرد. با استفاده از یک تحلیل‌گر داده‌های شبکه، کلیهٔ اطلاعات جذب‌شده، تجزیه‌وتحلیل می‌شود و کلیهٔ رمزهای عبور و نام‌های کاربری شبکه استخراج می‌گردد.

پویش ورودی[3]: پویش‌کردن ورودی به‌وسیلهٔ نرم‌افزارهایی انجام می‌شود تا ورودی‌های باز سامانه مشخص شود. بعدازآن با پیداکردن نقاط آسیب‌پذیر ورودی‌های یادشده، یک حمله شکل می‌گیرد.[4] (www.niazisoft.blogfa.com)

مسائل عمدهٔ مرتبط با امنیت اینترنت و فضای سایبر: مسائلی که به نظر می‌رسد تمامی کشورها در رابطه با تلاش‌های امنیت اینترنت و فضای سایبری با آن مواجه هستند، شامل:

۱)اطمینان‌نداشتن از موقعیت جغرافیایی عاملان حملات اینترنتی

۲)ادغام در حال تحول دستگاه‌های فنّاوری تلفن همراه به زیرساخت‌های اطلاعاتی حساس

۳)آسیب‌پذیری‌های جدید به زیرساخت‌های کشور از تهدیدهای پیچیده و فزاینده

۴)ضعف هماهنگی بخش دولتی و خصوصی به خطرات در حال ظهور

۵)ابهامات قانونی برای پاسخ به این‌گونه حمله‌هاست (تئوهاری، ۲۰۰۹).

این مسائل دست‌کم چهار پیامد مهم را برای دولت‌های ملی در پی خواهد داشت:

۱. تغییر برداشت دولت‌ها دربارهٔ چگونگی تعریف منافع، پایگاه‌های قدرت و امنیتشان

۲. بالاگرفتن چالش‌هایی در برابر توانایی دولت‌ها برای اداره و واپایش انتشار اطلاعات (روزنا و دیگران، ۱۳۹۰: ۱۳۰).

۳. ارتباط موضوع امنیت با شبکه‌های جهانی

1. Dictionary
2. Dictionary
3. Port scanning
4. www.niazisoft.blogfa.com

۴.کـاهش ظرفیت دولت‌ها در تولید امنیت شهروندان خود (کلارک، ۱۳۸۶: ۲۴۳).

ضریب عملکرد امنیتی شبکهٔ اینترنت: امنیت ملی امروزه با تهدیدهای بی‌شماری مواجه است؛ اما در این میان، تهدیدهای سایبری و رایانـه‌ای پدیـدهٔ جدیـدی اسـت کـه همـراه بـا فنّـاوری اطلاعات و گسترش ارتباطات گریبانگیر دولـت‌هـا شده است. این پدیده آن‌قدر جدید است کـه بررسی پیامدهای آن برای امنیت ملی دولـت‌هـا تـا حد زیادی مورد غفلت واقع شده اسـت. در دو دههٔ اخیر یک طیف، گرایش بـه زیـر سـؤال بـردن رویکـرد رایجـی کـه دربـارهٔ امنیـت در چارچوب مطالعات راهبـردی در طـول دورهٔ جنـگ سـرد توسعه داده شـده اسـت، دارنـد. ایـن گرایش تأکید بر ضـرورت فراگرفتن ازآنچه در بسـیاری از نگرش‌ها به‌عنوان تفسـیر بـیش‌ازحـد نظامی شده از امنیت در نظر گرفته شده و ملازم با ظهـور چالش‌های امنیتی جدید بوده اسـت، دارد (کلارک، ۱۳۸۶ :۲۳۶). از نظر این گروه، امروزه دیگر تهدیدهای امنیتی صرفاً نظـامی نیسـت؛ بلکه مسائل زیست‌محیطی، فقر جهانی، مهاجرت و اخیراً تهدیدهای سایبری و رایانه‌ای بـیش از تهدیدهای نظامی، امنیت دولت‌ها را به خطر انداخته است. در بهترین حالت باید بتوان از شبکه در مقابل تمامی انواع خطا محافظت کرد؛ اما امنیت ارزان به دست نمی‌آید؛ بنابراین باید ارزیابی مناسبی را بر روی انواع خطرات انجام داد تا مهم‌ترین آن‌ها را تشخیص دهیم و از طـرف دیگـر منابعی که باید در مقابل این خطرات محافظت شوند نیز شناسـایی شـوند. دو مؤلفـهٔ اصـلی در تحلیل اهداف امنیتی در شبکهٔ اینترنت عبارتند از: احتمال انجام حمله، خسارت وارده به شبکه در صورت انجام حملهٔ موفق.

درهرحال شکل و نوع طراحی سامانهٔ امنیتی یک شبکهٔ ارتباطی در مواجهه با حملات، بیشترین تأثیر را داشته و چنانچه این طراحی دربرگیرندهٔ همهٔ لایه‌های شبکهٔ ارتباطی اعـم از: پیرامـون، شبکه، میزبان، برنامهٔ کاربردی و دیتا، باشد هم یک راهبرد فنی است که ابزار و امکان مناسـبی را در سطوح مختلف در زیر ساختار شبکهٔ شما قرار می‌دهد و هم یک راهبرد سـازمانی خواهـد بود که مشارکت همه را می‌طلبد. هدف در اینجا ایجاد درکی در سطح پایـه از امنیـت شـبکه و پیشنهاد یک رویکرد عملی مناسـب بـرای محافظـت از امکانـات ارتبـاطی اسـت. محافظـت از اطلاعات اختصاصی، به منابع مالی نامحدود و عجیب و غریب نیاز ندارد. با درکی کلی از مسئله، خلق یک طرح امنیتی راهبردی و راهکنشی می‌تواند تمرینی آسان باشد. افزون برآن، با رویکرد عملی که در اینجا معرفی می‌شود، می‌توانید بدون هزینه‌کردن بودجه‌های کلان، موانـع مـؤثری بر سر راه اخلال‌گران امنیتی ایجاد کرد. متخصصان امنیت شبکه از اصطلاحی با عنوان ضـریب

عملکرد[1] استفاده می‌کنند که مفهومی مهم در پیاده‌سازی امنیت شبکه است. ضریب عملکرد به‌عنوان میزان تلاش موردنیاز توسط یک نفوذگر برای تحت تأثیر قرار دادن یک یا بیشتر از سامانه‌ها و ابزار امنیتی تعریف می‌شود که باعث رخنه‌کردن در شبکه می‌شود. یک شبکه با ضریب عملکرد بالا به‌سختی مورد دستبرد قرار می‌گیرد. درحالی‌که یک شبکه با ضریب عملکرد پایین می‌تواند نسبتاً به‌راحتی مختل شود. اگر هکرها تشخیص دهند که شبکه ضریب عملکرد بالایی دارد که فایدهٔ رویکرد لایه‌بندی شده نیز هست، احتمالاً شبکهٔ شمارا رها می‌کنند و به سراغ شبکه‌هایی با امنیت پایین‌تر می‌روند و این دقیقاً همان چیزی است که شما می‌خواهید. در الگوی امنیت مبتنی بر بستر ساختار شبکه بعضی از فنّاوری‌های تدافعی که در هر سطح مورد استفاده قرار می‌گیرند، در جدول زیر ارائه شده‌اند.

جدول شماره ۲-سطوح امنیتی

ردیف	سطح امنیتی	فنّاوری امنیتی قابل‌استفاده
۱	پیرامون	فایروال، آنتی‌ویروس در سطح شبکه، رمزنگاری شبکهٔ خصوصی مجازی
۲	شبکه	تشخیص/جلوگیری از نفوذ IDS/IPS،va، تبعیت امنیتی کاربر انتهایی، واپایش دسترسی/ تأیید هویت کاربر
۳	میزبان	نظام تشخیص نفوذ میزبان، نظام ارزیابی آسیب‌پذیری میزبان، تبعیت امنیتی کاربر انتهایی، آنتی‌ویروس واپایش دسترسی/ تأیید هویت کاربر
۴	برنامهٔ کاربردی	نظام تشخیص نفوذ میزبان، نظام ارزیابی آسیب‌پذیری میزبان، واپایش دسترسی/ تأیید هویت کاربر تعیین درستی
۵	داده	رمزنگاری، واپایش دسترسی/ تأیید هویت کاربر

منبع: (www.niazisoft.blogfa.com)

اقدام پیشگیرانهٔ امنیتی در شبکهٔ اینترنت:

معماری امنیتی: با توجه به ساختار هر شبکه، معماری امنیتی شبکه به‌صورت نهفته در لایه‌های شبکه در نظر گرفته می‌شود و لایه‌بندی با توجه به محدوده‌های داخلی، خارجی، ارتباط از راه دور و ... به‌صورت یک معماری امنیتی چهار لایه تعیین می‌گردد که عبارتند از: امنیت زیرساخت که شامل: پیکربندی دقیق تجهیزات شبکه است. امنیت ارتباطات که در آن با استفاده از

1. work factor

فایروال‌ها، سامانه‌های آی پی اس[1]، آی دی اس[2]، ضدویروس‌ها، سرورهای تری ای[3]، نرم‌افزارهـای پایشگر، ثبت و تحلیل رویدادها می‌توان به تشخیص هویت و واپایش کاربران پرداخت.[4]

۱) امنیت سامانه‌ها که در آن با بهره‌گیری از پویشگرهای امنیتی، آنتی‌ویروس‌هـا، آی دی اس و آی پی اس به ثبت و واپایش دسترسی کاربران به منابع پرداخته می‌شود.

۲) امنیت کاربران که با بهره‌گیری از سامانه‌های آی دی اس، آنتـی‌ویـروس، پویشـگر امنیتـی و فیلترهای محتوا بر دسترسی کاربران نظارت می‌شود (رئیسی، ۱۳۹۱: ۹).

راهکارهای امنیت اطلاعات: راهکارهای امنیت اطلاعات به دودسته تقسیم می‌شود:

الف) فنّاوری‌های امنیت اطلاعات کنش‌نمایانه یا کنشی؛ انجام عملیات پیشگیرانه قبـل از رخـداد یک مشکل خاص امنیتی است. درواقع جواب سؤال چه‌کـار بایـد انجـام دهـیم تـا ...؟ اسـت کـه به‌شرط زیر است.

۱. رمزنگاری: نوعی نوشتن پنهان و علم حفاظت، اعتمادپذیری و تأمین تمامیت داده‌هاست کـه شامل سه مرحلهٔ رمزگذاری، رمزگشایی و تحلیل رمز است. کدگذاری واژه‌ها به‌صورت پنهـان را رمزگذاری گویند و بازیابی متن آشکار (پیام) از متن رمزی را رمزگشایی می‌نامند. الگوهای رمزگذاری و رمزگشایی توسط دو روش انجام می‌گردد:
   - الگوی متقارن: که استفاده از کلیدهای یکسانی برای رمزگذاری و رمزگشایی است.
   - الگوی ناهم‌تراز: استفاده از کلیدهای متفاوت برای رمزگذاری و رمزگشایی است. بازیـابی متن آشکار بدون کلید مناسب را تحلیل رمز گویند.
۲. امضاهای رقومی: معادل «امضای دست‌نوشت» و همان هدف را دارد. نشانهٔ منحصربه‌فرد یک شخص است؛ بنابراین نباید جعل‌شدنی باشد.
۳. شبکه‌های مجازی خصوصی: فنّاوری شبکه‌هـای مجـازی خصوصـی، عبـور و مـرور شـبکه را رمزگذاری می‌کند؛ بنابراین این فنّاوری برای تضمین درستی و امنیت داده‌ها، بـه رمزنگـاری

1. Intrusion Prevention System
2. Intrusion Detection System

۳. AAA Server یک برنامه نرم افزاری سرور است که امکان دسترسی کاربران را با منابع رایانه شبکه برقـرار مـی‌کنـد. ایـن برنامـه بـرای شـبکه‌هـای Enterprise سرویس‌های Authentication ، Authorization و Accounting را فراهم می‌آورد.

۴. IDS یک سامانهٔ محافظتی است که خرابکاری‌های در حال وقوع روی شبکه را شناسایی می‌کند. روش کار بـه ایـن صـورت اسـت کـه بـا اسـتفاده از تشخیص نفوذ که شامل مراحل جمع آوری اطلاعات، پویش ورودی‌ها، به دست آوری واپایش رایانه‌ها و نهایتاً هک کردن است، می‌تواند نفوذ خرابکاری‌ها را گزارش و کنترل کند.

سامانه جلوگیری از نفوذ (IPS) یک وسیله امنیتی است که بر فعالیت‌های یک شبکه و یا یک سامانه نظارت کرده تا رفتارهـای ناخواسـته یـا مخـرب را شناسایی کند. در صورت شناسایی این رفتارها، بلافاصله واکنش نشان داده و از ادامه فعالیت آن‌ها جلوگیری می‌کند. سامانه‌های جلوگیری از نفوذ به سـه دسته مبتنی بر میزبان و مبتنی بر شبکه و مبتنی بر برنامه تقسیم می‌شوند.

وابسته است. این شبکهٔ بسیار امن، برای انتقال داده‌های حساس (ازجمله اطلاعات تجاری الکترونیکی) از اینترنت به‌عنوان رسانهٔ انتقال بهره می‌گیرد.

۴. نرم‌افزارهای آسیب‌نما: برنامه‌هایی برای بررسی نقاط ضعف یک شبکه یا نظام یا وبگاه هستند. بدین معنا که میزبان‌های روی شبکه در فواصل نامنظم پویش می‌شوند. به‌محض خاتمه‌یافتن بررسی یک میزبان از داده‌های آن نمونه‌برداری می‌شود. درواقع یک عکس فوری گرفته می‌شود.

۵. پویشگرهای ضدویروس: برنامه‌های نرم‌افزاری هستند که برای بررسی و حذف ویروس‌های رایانه‌ای، طراحی‌شده‌اند. کارهایی که انجام می‌دهند عبارتنداز:

- پیشگیری از فعالیت ویروس
- حذف ویروس
- تعمیر آسیبی که ویروس عامل آن بوده است.
- گرفتن ویروس در زمان واپایش و بعد از فعال شدن آن.

۶. پروتکل‌های امنیتی: شیوه‌های استاندارد که تبادل اطلاعات را میان سامانه‌ها، واپایش و هدایت می‌کنند.

۷. سخت‌افزارهای امنیتی: ابزارهای فیزیکی؛ مانند امنیت سرورها، امنیت کابل‌ها و غیره که کاربرد امنیتی دارند.

۸. جعبه‌های توسعه نرم‌افزار امنیتی[1]: ابزارهای برنامه‌نویسی؛ مانند «مدیریت امنیت جاوا»[2] که در ایجاد برنامه‌های امنیتی و ساختن برنامه‌های کاربردی امنیتی کاربرد دارند (قاسمی، ۱۳۸۶ :۱۰-۹).

ب) فنّاوری‌های امنیت اطلاعات واکنشی: انجام واکنش لازم پس از رخداد یک مشکل خاص امنیتی است. درواقع پاسخ سؤال (اکنون‌که ... چه‌کار باید انجام دهیم؟) که به‌شرح زیر است:

۱. دیوار آتش: اولین خط دفاعی برای دفع مزاحم است. دیوار آتش یک فیلتر بین سازمان داخلی (امین) و اینترنت (غیر امین) نصب می‌شود و هدف آن جلوگیری از ارتباطات غیرمجاز در درون یا بیرون شبکه داخلی میزبان است.

۲. واپایش دسترسی: مجموعه سیاست‌های مربوط به اجازه دادن یا اجازه ندان برای دسترسی یک کاربر خاص به قسمت‌های مختلف اطلاق می‌شود.

1. security software development kits
2. manager security Java

۳. کلمات عبور: کلمه یا عبارتی است که فرد برای دریافت مجوز دسترسی به اطلاعات باید وارد نماید.
۴. زیست‌سنجی: علم سنجش و تحلیل داده‌های زیستی است. در امنیت اطلاعات، از تحلیل ویژگی‌های بدن انسان (مانند اثرانگشت، قرنیه و شبکیهٔ چشم، ساختارهای صدا، ساختارهای چهره و اندازه‌های دست) برای تعیین اعتبار استفاده می‌شود.
۵. سامانه‌های آشکارساز نفوذی: یک نظام دفاعی است که فعالیت‌های مخاطره‌آمیز را در یک شبکه تشخیص می‌دهد. از ویژگی‌های مهم آن، توانایی در تأمین نمایی از فعالیت‌های غیرعادی و اعلام هشدار به مدیران و مسدود نمودن ارتباط مشکوک است.
۶. واقعه‌نگاری: به ثبت نظام‌مند رویدادهای مشخص به ترتیب رخداد آن‌ها برای فراهم‌کردن امکان تعقیب و پیگیری داده‌ها در تحلیل‌های آتی اطلاق می‌شود.
۷. دسترسی از راه دور: دسترسی به یک نظام یا برنامه، بدون نیاز به حضور فیزیکی در محل است که خطر جعل هویت در آن‌ها بیشتر است. به همین دلیل معمولاً واپایش‌شده نیستند (قاسمی، ۱۳۸۶ :۱۱).

تعاریف امنیت: تعاریف مندرج در فرهنگ‌های لغت دربارهٔ مفهوم کلی امنیت، بر روی «احساس آزادی از ترس» یا «احساس ایمنی» که ناظر بر امنیت مادی و روانی است، تأکیددارند (مندل، ۱۳۷۹: ۴۴). چندبعدی بودن مفهوم امنیت ملی سبب شده است دیدگاه‌های بسیار متنوعی راجع به آن وجود داشته باشد و هرکسی از زاویه دید خود به تعریف آن بپردازد. در همین راستا، برخی از نظریه‌پردازان، امنیت ملی را معادل باارزش‌های حیاتی کشور می‌دانند، بدان گونه که آرنولد ولفرز آن را برابر با «نبود تهدید برای ارزش‌های اکتسابی» می‌داند (ولفرز، ۱۹۶۲: ۱۵۰). باری بوزان نیز امنیت را «رهایی از تهدید و توانایی دولت و جوامع برای حفظ هویت مستقل و یک‌پارچگی کارکردی در مقابل نیروی تغییردهنده» تعریف می‌کند (بوزان، ۱۳۷۸: ۴۳۲). درعین‌حال، یکی از کامل‌ترین تعاریف را ریچارد اولمن ارائه کرده است: «تهدید امنیت ملی اقدام یا سلسله رویدادهایی است که نخست، به شکلی مؤثر و در دوره زمانی کوتاه خطر کاهش کیفیت زندگی را برای ساکنان کشور پیش آورد و دوم با خطر جدی کاهش طیف خط‌مشی‌هایی که حکومت یا واحدهای غیر حکومتی خصوصی موجود در داخل کشور (اشخاص، گروه‌ها، شرکت‌ها) می‌توانند از میان آن‌ها دست به انتخاب بزنند، همراه باشد. مسلماً با این تعریف تصور ما از عوامل تهدیدزا دامنهٔ بیشتری می‌یابد» (تریف، ۱۳۸۳:۴۹).

انواع امنیت:

امنیت فیزیکی: با توجه به اینکه هرگونه طرح امنیتی با وجود دسترسی فیزیکی، شکستنی است، در حوزه‌های زیر بررسی‌های کارشناسی لازم صورت گرفته و گزارشی برای برطرف نمودن آن‌ها به مدیر شبکه ارائه می‌گردد: امنیت فیزیکی سرورها، سوئیچ‌ها، روترها و فایروال‌ها؛ امنیت فیزیکی ایستگاه‌های کاری؛ امنیت فیزیکی ارتباطات سیمی و بی‌سیم.

۱) امنیت سرورها: در هر سازمان، سرور یا سرورهایی برای ارائه سرویس‌های مختلف به کاربران وجود دارد. بدین‌سبب باید با در نظرگرفتن تنظیمات امنیتی خاص مانع از ایجاد اخلال در فعالیت‌های مهم آن‌ها شویم.

۲) امنیت ایستگاه‌های کاری: یکی از مهم‌ترین دلایل بروز مشکلات امنیتی، رایانه‌های کاربرانی است که بدون تنظیمات امنیتی لازم در شبکه مشغول به کار هستند. درنتیجه باید بر روی تمام ایستگاه‌های کاری تنظیمات امنیتی خاص اعمال شود و افزون‌برآن، تنظیمات امنیتی نیز از طریق سرور بر روی این ایستگاه‌های کاری به‌صورت خودکار انجام گیرد.

۳) امنیت ارتباطات: نشت اطلاعات سازمانی از مهم‌ترین تهدیدات امنیتی است. درنتیجه باید با پیکربندی مناسب، تمام ارتباطات؛ ازجمله ارتباطات بی‌سیم سازمان امن شود و ارتباطاتی که بستر آن شبکه‌های ناامنی؛ مانند اینترنت است، به‌صورت رمزنگاری با استفاده از پروتکل‌های امنیتی ایمن‌سازی گردند.

۴) امنیت ساختار شبکه: در صورت اصلاح نشدن ساختار شبکه، همیشه مشکل ناامنی باقی می‌ماند. درنتیجه باید با ایجاد ناحیهٔ مناسب، جداسازی نواحی مختلف؛ مانند شبکهٔ اینترنت، سرورها، ایستگاه‌های کاری و ... انجام پذیرد. برای جلوگیری از حملات و دسترسی‌های غیرمجاز، باید ترافیک عبوری بین این نواحی توسط فایروال‌ها واپایش گردد.

۵) مستندسازی خط‌مشی‌ها و دستورکارهای امنیتی: مهم‌تر از ایجاد امنیت در شبکهٔ سازمان، حفظ و تداوم امنیت است. ازاین‌رو اطلاعاتی؛ مانند نقشه‌های منطقی و فیزیکی شبکه، کابل‌کشی، پیکربندی تجهیزات و سامانهٔ عامل‌ها، مستند خواهد شد. هم‌چنین باید دستورکارهایی برای نگهداری و بازبینی تجهیزات و سرویس‌ها و فعالیت‌های مرتبط با شبکهٔ سازمان؛ مانند پشتیبان ارائه گردد.

۶) نظارت امنیتی: برای اطمینان از عملکرد درست نظام، باید ابزار و آموزش لازم برای مدیر شبکهٔ سازمان برای پویش و واپایش شبکه و بررسی و تحلیل لاگ‌ها ارائه شود.

۷) آموزش و فرهنگ‌سازی: با توجه به نقش مهم کارکنان سازمان در حفظ امنیت شبکه و اطلاعات سازمان، آموزش‌های لازم برای ارتقای سطح دانش فنی در مورد مسائل امنیتی، با

برگزاری دوره‌های آموزشی در دو سطح راهبران و کاربران در سازمان انجام می‌گردد (رئیسی، ۱۳۹۱: ۴-۳).

امنیت اطلاعات: امنیت اطلاعات به محرمانگی، یک‌پارچگی و در دسترس‌بودن داده‌ها مربوط است. بدون در نظر گرفتن فرم اطلاعات اعم از الکترونیکی، چاپ و یا اشکال دیگر.

محرمانگی؛ یعنی جلوگیری از افشای اطلاعات به افراد غیرمجاز. برای مثال، برای خرید با کارت‌های اعتباری بر روی اینترنت نیاز به ارسال شمارهٔ کارت اعتباری از خریدار به فروشنده و سپس به مرکز پردازش معامله است. در این مورد شمارهٔ کارت و دیگر اطلاعات مربوط به خریدار و کارت اعتباری او نباید در اختیار افراد غیرمجاز بیفتد و این اطلاعات باید محرمانه بماند. در این مورد برای محرمانه نگه‌داشتن اطلاعات، شمارهٔ کارت رمزنگاری می‌شود و در طی انتقال یا جاهایی که ممکن است ذخیره شود (در پایگاه‌های داده، پوشه‌های ثبت وقایع نظام، پشتیبان‌گیری، چاپ رسید و غیره) رمزشده باقی می‌ماند. هم‌چنین دسترسی به اطلاعات سامانه‌ها نیز محدود می‌شود. اگر فردی غیرمجاز به شمارهٔ کارت به هر نحوی دست یابد، نقض محرمانگی رخ داده است. نقض محرمانگی ممکن است اشکال مختلف داشته باشد. مثلاً اگر کسی از روی شانهٔ شما اطلاعات محرمانهٔ نمایش‌داده شده روی صفحهٔ نمایش رایانهٔ شما را بخواند؛ یا فروش یا سرقت رایانهٔ لپ‌تاپ حاوی اطلاعات حساس؛ یا دادن اطلاعات محرمانه از طریق تلفن، همه موارد نقض محرمانگی است.

یک‌پارچه بودن: یک‌پارچه بودن؛ یعنی جلوگیری از تغییر داده‌ها به‌طور غیرمجاز و تشخیص تغییر در صورت دست‌کاری غیرمجاز اطلاعات. یک‌پارچگی وقتی نقض می‌شود که اطلاعات در حین انتقال به‌صورت غیرمجاز تغییر داده می‌شود. سامانه‌های امنیت اطلاعات به‌طور معمول افزون‌بر محرمانه بودن اطلاعات، یک‌پارچگی آن را نیز تضمین می‌کنند.

دسترس‌پذیر بودن: اطلاعات باید زمانی که موردنیاز توسط افراد مجاز هستند در دسترس باشند. این بدان معنی است که باید از درست کارکردن و جلوگیری از اختلال در سامانه‌های ذخیره و پردازش اطلاعات و کانال‌های ارتباطی مورد استفاده برای دسترسی به اطلاعات اطمینان حاصل کرد. سامانه‌های با دسترسی بالا در همه حال حتی به علت قطع برق، خرابی سخت‌افزار و ارتقای سامانه در دسترس باقی می‌ماند. یکی از راه‌های از دسترس خارج کردن اطلاعات و سامانه اطلاعاتی درخواست بیش‌ازاندازه از طریق خدمات از سامانهٔ اطلاعاتی است که در این حالت چون سامانه توانایی و ظرفیت چنین حجم انبوه خدمات‌دهی را ندارد از سرویس دادن به‌طور کامل یا جزئی عاجز می‌ماند. (http://iedco.ir/article)

مؤلفه‌های پیشگیرانه مؤثر در شبکهٔ اینترنت:

آموزش و مهارت افزایی کاربران شبکه: بدون تردید، کارشناسان آموزش‌دیده و خبره، یکی از منابع ارزشمند در هر سازمان محسوب می‌گردند. همواره می‌بایست از کارشناسان ورزیده در ارتباط با امنیت در یک سازمان استفاده گردد. استفاده از یک کارشناس غیرماهرانه در امور امنیت اطلاعات و شبکه در یک سازمان، خود تهدیدی امنیتی است که بر سایر تهدیدات موجود اضافه خواهد شد. ما نمی‌توانیم مسئولیت پیاده‌سازی راهبرد امنیتی در سازمان را به افرادی واگذار نماییم که در این رابطه اطلاعات و دانش لازم را ندارند. وجود ضعف امنیتی در شبکه‌های رایانه‌ای و اطلاعاتی، نبود آموزش و توجیه درست تمامی کاربران، نبود دستورکارهای لازم برای پیش‌گیری از نقایص امنیتی، نبود سیاست‌های مشخص و مدون برای برخورد مناسب و به‌موقع با اشکالات امنیتی، مسائلی را در پی خواهد داشت که ضرر آن متوجه تمامی کاربران رایانه در یک کشور می‌شود و در عمل زیرساخت اطلاعاتی یک کشور را در معرض آسیب و تهدید جدی قرار می‌دهد. (www.monazam.ir)

بومی‌سازی تجهیزات و نرم‌افزارها (واپایش تجهیزات غیربومی، به‌کارگیری نرم‌افزار بومی، تولید سخت‌افزار بومی)

آینده‌پژوهی سایبری: آینده‌پژوهی دانشی است که می‌کوشد در درجه اول بر اساس یک سری رویکردهای اکتشافی آینده‌های مختلف، آینده‌های بدیل را کشف و شناسایی بکند. در این رویکرد هیچ هنجاری نیست؛ یعنی شما به‌صورت منفعل[1] در انتظار این هستید که برخی از این آینده‌هایی را که پیش‌بینی کردید به رخداد بپیوندد. این؛ یعنی فقط فهم این‌که آینده چه خواهد بود و رویکرد دیگر این است که آینده‌پژوهی می‌کوشد آینده را نه در قالب یک آینده مشخص و قطعی و دترمینیستی؛ بلکه آینده‌ای بدیل بشناسد و یک قسمت هم آینده‌پژوهی هنجاری[2] است که آینده‌پژوهی بعد از این‌که با آینده‌ها آشنا شد به آینده مطلوب فکر می‌کند؛ یعنی درواقع، ساختن و معماری آینده‌ای که مطلوب ما است. این رویکرد هنجاری است؛ یعنی رفتار طلب می‌کند و از طرفی به‌شدت ارزشی است. ارزش بنیاد است؛ یعنی آیندهٔ مطلوب من با شما ممکن است بسیار متفاوت باشد و به خاطر همین در اینجا موضوع ارزش‌ها بسیار مهم هستند. یکی از شارحان بزرگ آینده‌پژوهی که کتاب تحت عنوان بنیان‌های آینده‌پژوهی تألیف نموده است، اعتقاد دارد که آینده‌پژوهی یک رویکرد و سنت غربی نیست و این را هم حتماً

1. passive
2. normative

توجه داشته باشید که آینده‌پژوهی در هر منطقه‌ای از جهان به شکل بومی در حال تغییر و تحول است. ایشان می‌گوید ما منتظر نواهای تازه و نگرش‌های جدید در ساحت و عرصه آینده‌پژوهی هستیم (خزائی؛۱۳۹۰/۰۵/۱۲).

مؤلفه‌های اقدام تدافعی در شبکهٔ اینترنت:

پایش مستمر و مؤثر شبکه (تشخیص نفوذ): به‌طورمعمول، ابتدایی‌ترین خطوط دفاعی ما در مقابل حملات اینترنتی، استفاده از دیواره‌های آتش[1] و به‌روز نگاه‌داشتن و استفاده از آخرین نسخه برنامه‌ها (با توجه به گفته بالا اگر برنامه قدیمی نبوده و قابلیت به‌روزرسانی داشته باشد) است. همچنین استفاده هم‌زمان از سامانه‌های تشخیص نفوذ/ جلوگیری از نفوذ[2] نیز می‌تواند بسیار مفید باشند که درنهایت به ارتقای سطح امنیت می‌انجامد. در بسیاری از موارد، مهاجمان و نفوذگران با ابزارهایی شبیه ورودی پویشگرها در ابتدا به جمع‌آوری اطلاعات از شبکهٔ هدف پرداخته و اطلاعات مواردی نظیر ورودی‌های باز، سرویس‌های در حال اجرا و نرم‌افزارهای در حال استفاده را استخراج می‌نمایند. سپس نسبت به پیدا نمودن آسیب‌پذیری در نرم‌افزار و یا سرویس‌های در حال اجرا اقدام نموده و آنگاه به دور زدن سامانه از روش‌هایی؛ مانند سرریز بافر و یا استفاده از آسیب‌پذیری‌ها؛ مانند حملاتی شبیه «روز صفر»[3] مبادرت می‌کنند و ممکن است نقص و حفره موجود در سامانه موجب نقض یکی از موارد محرمانگی، یک‌پارچگی و یا در دسترس بودن گردد. هم‌چنین مهاجمین می‌توانند با تغییر مبدأ آی پی خود[4]، منشأ بسته را عوض نموده و با دست‌کاری بسته‌ها، محتوای دلخواه و مخرب خود را در داخل آن پنهان کرده و با ارسال آن دیواره‌های آتش را دور بزنند؛ بنابراین باز کردن ورودی توسط هریک از سرویس‌ها و باز گذاشتن دائمی یک ورودی، به‌عنوان یک تهدید در نظر گرفته می‌شود. درنتیجه، نظارت و واپایش دسترسی به ورودی‌ها می‌تواند تضمینی اعتمادپذیر جهت داشتن اتصال و ارتباطی امن باشد و به دنبال آن در ابتدایی‌ترین سطح در لبه شبکه افزون‌بر سامانه‌هایی نظیر دیوارهٔ آتش، به سازوکارهای خوب و قوی‌تر دیگری نیز نیاز داریم. یکی از این سازوکارها احراز هویت است. راه‌ها و روش‌های زیادی جهت ایجاد سرویس‌های احراز هویت برای افزایش لایه‌های امنیتی وجود دارند (پور وهاب، ۱۳۹۴: ۲۶). بیشتر شبکه‌های امروزی در ورای پیرامون، باز

1. Firewall
2 . IPS/IDS
3. day-zero
4. Address IP Source

هستند؛ یعنی هنگامی‌که داخل شبکه قرار دارید، می‌توانید به‌راحتی در میان شبکه حرکت کنید که به‌این‌ترتیب این شبکه‌ها برای هکرها و افراد بداندیش به اهدافی وسوسه‌انگیز مبدل می‌شوند. فنّاوری‌های زیر امنیت را در سطح شبکه برقرار می‌کنند. برای مقابله با نفوذکنندگان ای به سامانه‌ها و شبکه‌های رایانه‌روش‌های متعددی تدوین شده که روش‌های تشخیص نفوذ نامیده می‌شوند. هدف از تشخیص نفوذ این است که استفاده غیرمجاز و سوءاستفاده از شبکه‌های رایانه‌ای توسط هردو دستهٔ کاربران داخلی و حمله‌کنندگان خارجی آسیب‌رسان به سامانه‌ها شناسایی شوند. «سامانه‌های تشخیص نفوذ»[1] و «سامانه‌های جلوگیری از نفوذ»[2]: فنّاوری‌های آی.دی. اس و آی.پی.اس ترافیک گذرنده در شبکه را با جزئیات بیشتر نسبت به فایروال تحلیل می‌کنند. مشابه سامانه‌های آنتی‌ویروس، ابزارهای آی.دی. اس و آی.پی.اس ترافیک را تحلیل و هر بسته اطلاعات را با پایگاه دادهای از مشخصات حملات شناخته شده مقایسه می‌کنند .هنگامی‌که حملات تشخیص داده می‌شوند، این ابزار وارد عمل می‌شوند. ابزارهای آی.دی. اس مسئولان را از رخداد یک حمله مطلع می‌سازند؛ ابزارهای آی.پی.اس یک گام جلوتر می‌روند و به‌صورت خودکار ترافیک آسیب‌رسان را مسدود می‌کنند. آی.دی. اس ها و آی.پی.اس ها مشخصات مشترک زیادی دارند، در اصل بیشتر آی.پی.اس ها در هسته خود یک آی.دی. اس دارند. تفاوت کلیدی بین این فنّاوری‌ها این است که محصولات آی.دی. اس تنها ترافیک آسیب رسان را تشخیص می‌دهند، درحالی‌که محصولات آی.پی.اس از ورود چنین ترافیکی به شبکه شما جلوگیری می‌کنند آی.دی. اس یک سامانه محافظتی است که خرابکاری‌های در حال رخداد روی شبکه را شناسایی می‌کند .روش کار به این صورت است که با استفاده از تشخیص نفوذ که شامل مراحل جمع‌آوری اطلاعات، پویش ورودی‌ها، به دست آوری واپایش رایانه‌ها و نهایتاً هک کردن است، می‌تواند نفوذ خرابکاری‌ها را گزارش و واپایش کند (جلیلی و مهدی‌آبادی، ۱۳۸۶: ۲۵۶)

برنامهٔ محافظ کاربردی: در حال حاضر امنیت سطح برنامه کاربردی بخش زیادی از توجه را معطوف خودکرده است. برنامه‌هایی که به میزان کافی محافظت نشده‌اند، می‌توانند دسترسی آسانی به دیتا و رکوردهای محرمانه فراهم کنند. حقیقت تلخ این است که بیشتر برنامه‌نویسان هنگام تولید کد به امنیت توجه ندارند. برنامه‌ها برای دسترسی مشتریان، شرکا و حتی کارمندان حاضر در محل‌های دیگر، روی وب قرار داده می‌شوند. این برنامه‌ها، می‌توانند هدف

1. IDS
2.IPS

خوبی برای افرادی که نیات بد دارند، باشند؛ بنابراین بسیار مهم است که یک راهبرد امنیتی جامع برای هر برنامه تحت شبکه اعمال شود. فنّاوری‌های زیر امنیت را در سطح برنامه فراهم می‌کنند

- پوشش محافظ برنامه – از پوشش محافظ برنامه به‌کرات به‌عنوان فایروال سطح برنامه یاد می‌شود و تضمین می‌کند که تقاضاهای وارد شونده و خارج شونده برای برنامه مورد نظر مجاز هستند. یک پوشش که معمولاً روی سرورهای وب، سرورهای رایانامه، سرورهای پایگاه داده و ماشین‌های مشابه نصب می‌شود، برای کاربر شفاف است و با درجه بالایی با سامانه یکپارچه می‌شود.
- واپایش دسترسی/تصدیق هویت؛ مانند تصدیق هویت در سطح شبکه و میزبان، تنها کاربران مجاز می‌توانند به برنامه دسترسی داشته باشند.
- تعیین درستی ورودی؛ ابزارهای تعیین درستی ورودی بررسی می‌کنند که ورودی گذرنده از شبکه برای پردازش امن باشد. اگر ابزارهای امنیتی مناسب در جای خود مورداستفاده قرار نگیرند، هر تراکنش بین افراد و واسط کاربر می‌تواند خطاهای ورودی تولید کند. عموماً هر تراکنش با سرور وب شما باید ناامن در نظر گرفته شود؛ مگر اینکه خلافش ثابت شود.

مزایا: ابزارهای امنیت سطح برنامه، موقعیت امنیتی کلی را تقویت می‌کنند و اجازهٔ واپایش بهتری روی برنامه‌هایتان را می‌دهند. هم‌چنین سطح بالاتری از جواب‌گویی را فراهم می‌کنند؛ چراکه بسیاری از فعالیت‌های نمایش داده شده توسط این ابزارها، ثبت‌شده و قابل‌ردیابی هستند.

معایب: پیاده‌سازی جامع امنیت سطح برنامه، می‌تواند هزینه‌بر باشد؛ چراکه هر برنامه و میزبان آن باید به‌صورت مجزا ارزیابی، پیکربندی و مدیریت شود (www.ircert.com/articles/Layered).

پسورد و رمزنگاری[1]: به بیان ساده، رمزنگاری به معنای «نوشتن پنهان» و علم حفاظت، اعتمادپذیری و تأمین تمامیت داده‌هاست. این علم شامل اعمال رمزگذاری، رمزگشایی و تحلیل رمز است. امنیت سطح دیتا ترکیبی از سیاست امنیتی و رمزنگاری را دربر می‌گیرد. رمزنگاری دیتا، هنگامی‌که ذخیره می‌شود و یا در شبکه حرکت می‌کند. به‌عنوان روشی بسیار مناسب

1. Cryptography

است؛ زیرا چنانچه تمام ابزارهای امنیتی دیگر از کار بیفتند، یک طرح رمزنگاری قوی دیتای مختص شبکه را محافظت می‌کند (شریفی و رمضان زاده، ۱۳۸۰).

مراقبت‌های زیست‌شناخت: یک سامانهٔ زیست‌شناخت چند عامله سامانه‌ای است که در آن از بیش از یک مؤلفهٔ زیست‌شناخت برای تشخیص هویت استفاده می‌شود. سامانه‌های زیست‌شناخت باوجود امنیتی که ایجاد می‌کنند، دارای نقاط ضعفی هستند؛ ازاین‌رو استفاده از بیش از یک زیست‌شناخت برای افزایش ضریب امنیتی و کاهش درجهٔ خطا مورداستفاده قرار می‌گیرد. برای مثال، اثرانگشت یک فرد در طول زمان به‌ویژه برای افرادی که درگیر مشاغل خاصی؛ مانند کارهای ساختمانی که سخت هستند، ممکن است دچار آسیب شده و باعث شود دستگاه تشخیص هویت اثرانگشت درگرفتن تصویر و شناسایی با خطا مواجه شود. یکی دیگر از زیست‌شناخت‌های معروف و پرکاربرد چهره است که سال‌هاست مورد استفاده قرار می‌گیرد. در حقیقت، این روش قدیمی‌ترین روشی است که انسان‌ها از طریق آن خودشان را می‌شناسند. وجود وب‌کم در لپ‌تاپ و رایانه‌های جیبی امکان شناسایی چهرهٔ کاربران را امکان‌پذیر ساخته است. بااین‌وجود سامانهٔ تشخیص چهره به‌تنهایی دارای نقایصی است. مهم‌ترین عیب آن این است که چهره به‌آسانی می‌تواند دچار تغییر شود؛ حتی این تغییر می‌تواند به‌واسطهٔ چیزهایی مثل مو، عینک، کلاه و عمل جراحی پلاستیک و... اتفاق بیفتد که این امر قابلیت اطمینان امنیت زیست‌شناخت چهره را تاحد زیادی کاهش می‌دهد. زیست‌شناخت چهره به تغییرات نور، قیافه و ژست فرد نیز حساس است. به‌طورکلی، چهره باگذشت زمان تغییر می‌کند که این خود یک مشکل به‌حساب می‌آید. سامانه‌های تصدیق هویت خودکاری که تنها مبتنی براثر انگشت یا چهره هستند، بیشتر کارایی مورد انتظار را ندارند؛ ازاین‌رو در این مقاله برای شناسایی کاربر از ترکیب ویژگی‌های اثرانگشت و چهره استفاده می‌شود. با استفاده از سامانه‌های زیست‌شناخت چند حالتی، می‌توان محدودیت‌های سامانه‌های زیست‌شناخت تک‌حالتی را از بین برد. در سامانه‌های زیست‌شناخت چندحالتی، برای تصدیق هویت ویژگی‌های زیست‌شناخت متفاوتی برای تشخیص در نظر گرفته می‌شود و با این کار درستی، کارایی، اطمینان و میزان خطای سامانهٔ تصدیق هویت را بهبود می‌یابد. گفتنی است که سطح ترکیب ویژگی‌های زیست‌شناخت خود سه دسته‌اند:

۱. تلفیق در سطح به دست آوردن اطلاعات: چندین برداشت از بردار ویژگیِ روش‌های زیست‌شناخت مختلف استخراج شده و سپس به روش‌های مختلف باهم ترکیب می‌شوند.

۲. تلفیق در سطح حوزه تطابق: هر تطبیق زیست‌شناخت یک درجه شباهت ایجاد می‌کند که نشان‌دهندهٔ نزدیکی بردار ویژگی ورودی با بردار ساختار است که حوزهٔ تطابق نام دارد. در این سطح از تلفیق این حوزه‌ها می‌توانند باهم ترکیب شوند و در شناساندن کاربر به ما کمک می‌کنند.

۳. تلفیق در سطح تصمیم‌گیری: در این حالت هر زیست‌شناخت بر اساس اطلاعات و فن‌های خود عمل تشخیص را انجام می‌دهد. سپس بر اساس رأی‌گیری عمل تشخیص نهایی انجام می‌شود. شبکه‌های عصبی مصنوعی مورد استفاده در این مورد تمامی شبکه‌هایی هستند که در روش‌های قبل مورد استفاده قرارگرفته‌اند. درواقع در اینجا نیز می‌توان از ترکیبی از چند شبکهٔ عصبی مصنوعی استفاده کرد (اخوان صفار،۱۳۹۱: ۲۹۸).

تلهٔ سامانه‌ای[1]: تله‌های سامانه‌ای شبیه دیواره‌های آتش و یا سامانه‌های تشخیص ورود سرزده نیستند؛ بلکه یک سامانهٔ اطلاعاتی است که با استفاده از ارزش کاذب خود، اطلاعاتی راجع به فعالیت‌های بی‌مجوز و نامشروع جمع‌آوری می‌کند. تلهٔ سامانه‌ای مفهوم بسیار ساده‌ای دارد ولی دارای توانمندی‌هایی به شرح زیر است:

۱) داده‌های کوچک دارای ارزش فراوان را جمع‌آوری می‌کنند. به‌جای تولید ۱۰۰۰ زنگ خطر در یک روز آن‌ها فقط یک زنگ خطر را تولید می‌کنند، تله‌های سامانه‌ای فقط فعالیت‌های ناجور را ثبت می‌کنند و هر ارتباطی با تلهٔ سامانه‌ای می‌تواند یک فعالیت بدون مجوز و یا بداندیشانه باشد.

۲) ابزار راهکنشی جدید: تله‌های سامانه‌ای این‌گونه طراحی شده‌اند تا هر چیزی را که به سمت آن‌ها جذب می‌شود، با ابزارها و راهکنش‌های جدیدی که قبلاً دیده نشده‌اند،ذخیره کنند.

۳) کمترین احتیاجات: تله‌های سامانه‌ای به کمترین احتیاجات نیاز دارند؛ زیرا آن‌ها فقط فعالیت‌های یک رم[2] ناجور را به ثبت می‌رسانند؛ بنابراین با یک پنتیوم قدیمی و با ۱۲۸ مگابایت حافظهٔ اصلی به‌راحتی می‌توان آن را پیاده‌سازی کرد. انواع «تله‌های سامانه‌ای»: تله‌های سامانه‌ای کم‌واکنش که دارای ارتباط و فعالیتی محدود و تله‌های سامانه‌ای پرواکنش که معمولاً از راه‌حل‌های پیچیده‌تری استفاده می‌کنند؛ زیرا آن‌ها از سامانه عامل‌ها و سرویس‌های واقعی استفاده می‌کنند.

1. Honey pot
2. RAM

با عنایت به شرح اقدامات تدافعی که بیان شد، آنچه مسلم است تا سال ۱۹۹۰ سامانه‌های تشخیص نفوذ عمدتاً مبتنی بر میزبان بودند و دامنهٔ فعالیت خود را به رکوردهای ردیابی سامانهٔ عامل و یا سایر منابع اطلاعاتی با محوریت میزبان محدود می‌کردند. پویش امنیتی نت ورک (در دانشگاه کالیفرنیا) تشخیص نفوذ را به محیط شبکه گسترش داد. دی. آی. دی. اس[1] اولین تلاش برای تلفیق روش‌های تشخیص نفوذ مبتنی بر میزبان و شبکه بود؛ به‌گونه‌ای‌که یک گروه متخصص امنیتی می‌توانست تخطی‌های امنیتی و نفوذ از طریق شبکه را دنبال کند. دی. آی. دی. اس، از همکاری بین مرکز پشتیبانی رمز نیروی هوایی آمریکا، آزمایشگاه ملی دانشگاه کالیفرنیا، واحد دیویس و آزمایشگاه هایستیک[2] به وجود آمد. (جلیلی و مهدی‌آبادی،۱۳۸۰: ۲۶۴). دی. آی. دی. اس، اولین سامانه‌ای بود که با خودکارنمودن تعقیب و ارتباط شناسه‌های کاربران از طریق شبکهٔ نظارت‌شده، به استفاده‌کنندگان امکان می‌داد به این مسائل بپردازند. ... مراقبت مبنی بر میزبان از پوشه‌های رخدادهای سامانه‌عامل، برنامهٔ کاربردی و ترافیک شبکه، به‌عنوان منبع اصلی اطلاعات استفاده می‌کنند (جلیلی و مهدی‌آبادی، ۱۳۸۰:۲۶۶).

تجزیه‌وتحلیل داده‌ها

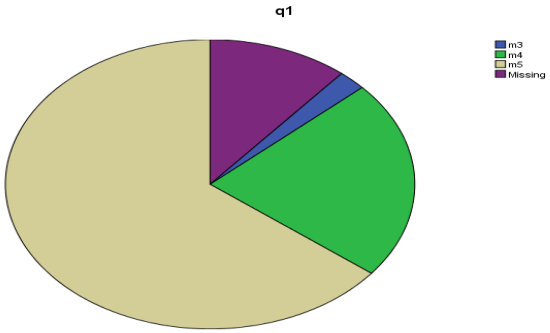
تجزیه‌وتحلیل توصیفی: در این بخش داده‌های استخراج‌شده از پرسش‌نامه به دو شکل توصیفی و استنباطی مورد تجزیه‌وتحلیل قرار می‌گیرند. ابتدا فرضیه‌های پژوهش بر اساس سؤال‌های پرسش‌نامه به شکل توصیفی مورد تجزیه‌وتحلیل قرار می‌گیرند و برای آن‌ها جداول توزیع فراوانی تشکیل می‌شود. این امر داده‌های پرسش‌نامه را به شکل منظمی سامان می‌دهد. در ادامه، داده‌ها به شکل استنباطی مورد تجزیه‌وتحلیل قرار می‌گیرند تا از این طریق به فرضیه‌های پژوهشی پاسخ داده شود.

فرضیهٔ یکم: اقدامات پیشگیرانه در قالب مهارت کاربران، واپایش تجهیزات، رمزنگاری دوره‌ای، نرم‌افزار بومی، سخت‌افزار بومی، سازمان‌دهی و تعادل سامانه و تحلیل محیط و آینده‌پژوهی سایبری در برقراری امنیت شبکهٔ اینترنت مؤثر است. داده‌های جدول (q1) حاکی از آن است که ۸۸ درصد پاسخ‌دهندگان معتقدند که اقدامات پیشگیرانه در حد خیلی زیاد و زیاد در برقراری امنیت شبکهٔ اینترنت مؤثر است.

[1]. distribiuted inrotion tetection system
[2]. haystake

جدول شماره ۳-فراوانی اقدامات پیشگیرانه

ارزش	فراوانی	درصد	درصد اعتبار	درصد کل
متوسط =m3	۱	۲.۲	۲.۵	۲.۵
زیاد =m4	۱۰	۲۲.۲	۲۵.۵	۲۷.۵
خیلی زیاد =m5	۲۹	۶۴.۴	۷۲.۵	۱۰۰.۰
کل	۴۰	۸۸.۹	۱۰۰.۰	
ازدست‌رفته	۵	۱۱.۱		
کل	۴۵	۱۰۰.۰		

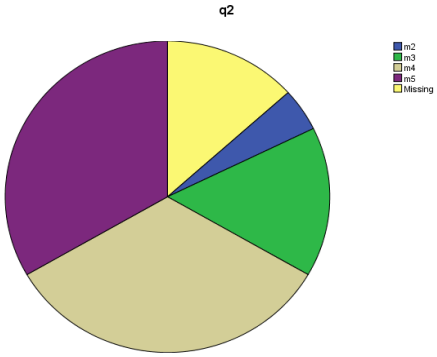


شکل شماره ۲-فراوانی اقدامات پیشگیرانه

فرضیهٔ دوم: اقدام تدافعی در قالب پایش مستمر شبکه، تلهٔ سامانه‌ای، رمزگذاری، شناسهٔ زیست‌شناخت و... در برقراری امنیت شبکهٔ اینترنت مؤثر است. داده‌های جدول (۲) حاکی از آن است که ۸۶.۷ درصد پاسخ‌دهندگان معتقدند که اقدامات تدافعی در حد خیلی زیاد و زیاد در برقراری امنیت شبکهٔ اینترنت مؤثر است.

جدول شماره ۴-فراوانی اقدامات تدافعی

ارزش	فراوانی	درصد	درصد اعتبار	درصد کل
کم =m2	۲	۴.۴	۵.۱	۵.۱
متوسط =m3	۷	۱۵.۶	۱۷.۹	۲۳.۱
زیاد =m4	۱۵	۳۳.۳	۳۸.۵	۶۱.۵
خیلی زیاد =m5	۱۵	۳۳.۳	۳۸.۵	۱۰۰.۰
کل	۳۹	۸۶.۷	۱۰۰.۰	
ازدست‌رفته	۶	۱۳.۳		
کل	۴۵	۱۰۰.۰		

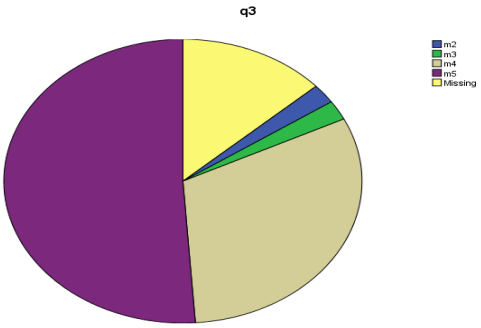


شکل شماره ۳-فراوانی اقدامات تدافعی

فرضیهٔ سوم: اقدامات تهاجمی در قالب هک مراکز حیاتی حریف، طراحی فریب سایبری در برقراری امنیت شبکهٔ اینترنت مؤثر است. داده‌های جدول (q3) حاکی از آن است که ۸۶.۶ درصد پاسخ‌دهندگان معتقدند که اقدامات تدافعی در حد خیلی زیاد و زیاد در برقراری امنیت شبکهٔ اینترنت مؤثر است.

جدول شماره ۵-فراوانی اقدامات تهاجمی

ارزش	فراوانی	درصد	درصد اعتبار	درصد کل
کم =m2	۱	۲.۲	۲.۶	۲.۶
متوسط =m3	۱	۲.۲	۲.۶	۵.۱
زیاد =m4	۱۴	۳۱.۱	۳۵.۹	۴۱.۰
خیلی زیاد =m5	۲۳	۵۱.۱	۵۶.۰	۱۰۰.۰
کل	۳۹	۸۶.۶	۱۰۰.۰	
ازدست‌رفته	۶	۱۳.۳		
کل	۴۵	۱۰۰.۰		



شکل شماره ۴-فراوانی اقدامات تهاجمی

مقایسه توصیفی مؤلفه‌های مرتبط با هریک از متغیرها که در معرض آراء جامعه خبره قرارگرفته‌اند نتایج زیر را دربرداشتن است: با نتایج به‌دست‌آمده برحسب میانگین استقبال جامعهٔ آماری از متغیرها، می‌توان آن‌ها را اولویت‌بندی نمود.

جدول شماره ۶-مقایسه توصیفی مؤلفه‌ها

مؤلفه‌ها	فراوانی	مینیمم	ماکزیمم	میانگین	انحراف معیار
مهارت کارکنان	44	2.00	5.00	4.2500	.94315
واپایش تجهیزات غیربومی	44	2.00	5.00	4.1591	.77589
رمزنگاری	45	3.00	5.00	4.4000	.61791
نرم‌افزار بومی	44	2.00	5.00	4.5455	.72991
سخت‌افزار بومی	45	1.00	5.00	4.2000	.94388
ساماندهی و تعادل	44	3.00	5.00	4.1591	.56828
آینده‌پژوهی	45	3.00	5.00	4.4000	.61791
هک مراکز حیاتی	45	1.00	5.00	4.1111	.74536
طرح فریب	44	3.00	5.00	4.2500	.71933
ضدویروس و ضدتروجان	45	2.00	5.00	4.0889	.82082
پایش مستمر	45	3.00	5.00	4.3333	.73855
ضد هکر	43	3.00	5.00	4.4651	.63053
تلهٔ سامانه‌ای	44	2.00	5.00	4.1364	.82380
رمز و کدگذاری	45	2.00	5.00	4.0444	.87790
شناسهٔ زیست‌شناخت	44	2.00	5.00	4.1818	.81477
Valid N (listwise)	33				

تجزیه‌وتحلیل استنباطی: برای آزمون فرضیه‌های پژوهش از آزمون آماری خی دو استفاده گردیده است.

فرضیهٔ یکم:

جدول شماره ۷-آمار استنباطی فرضیهٔ یکم

ارزش	مشاهده‌شده	مورد انتظار	باقی‌مانده
متوسط	۱	۱۳.۳	-۱۲.۳
زیاد	۱۰	۱۳.۳	-۳.۳
خیلی زیاد	۲۹	۱۳.۳	۱۵.۷
تعداد کل	۴۰		

جدول شماره ۸-آمار خی ۲ فرضیهٔ یکم

خی دو	۳۰.۶۵۰[a]
درجهٔ آزادی	۲
سطح معنی‌داری	.۰۰۰

همچنان که داده‌های جدول نشان می‌دهد، خی‌دوی محاسبه‌شده (۳۰.۶۵۰-) با درجهٔ آزادی df=2 معنی‌دار است. معنی‌داری خی‌دوی محاسبه‌شده به معنای تأیید فرض فرعی (۱) است. به عبارتی بین اقدامات پیشگیرانه در قالب مهارت کاربران، واپایش تجهیزات، رمزنگاری دوره‌ای، نرم‌افزار بومی، سخت‌افزار بومی، سازمان‌دهی و تعادل سامانه و تحلیل محیط و آینده‌پژوهی سایبری و امنیت شبکهٔ اینترنت رابطهٔ معناداری وجود دارد.

فرضیهٔ دوم:

جدول شماره ۹-آمار استنباطی فرضیهٔ دوم

ارزش	مشاهده‌شده	مورد انتظار	باقی‌مانده
کم	۲	۹.۸	-۷.۸
متوسط	۷	۹.۸	-۲.۸
زیاد	۱۵	۹.۸	۵.۲
خیلی زیاد	۱۵	۹.۸	۵.۲
کل	۳۹		

جدول شماره ۱۰-آماری ۲ فرضیهٔ دوم

خی دو	۱۲.۵۹۰
درجهٔ آزادی	۳
سطح معنی‌داری	.۰۰۰

همچنان که جدول نشان می‌دهد، خی‌دوی محاسبه‌شده (12.590-) با درجهٔ آزادی df=3 معنی‌دار است. معنی‌داری خی‌دوی محاسبه‌شده به معنای تأیید فرض فرعی (۲) است. به

عبارتی بین اقدامات تدافعی در قالب ضدویروس و ضدتروجان، ضد هکر، پایش مستمر شبکه، تلهٔ سامانه‌ای، رمزگذاری و شناسهٔ زیست‌شناخت و امنیت شبکهٔ اینترنت رابطهٔ معناداری وجود دارد.

فرضیهٔ سوم:

جدول شماره ۱۱-آمار استنباطی فرضیهٔ سوم

باقی‌مانده	مورد انتظار	مشاهده‌شده	ارزش
-۸.۸	۹.۸	۱	کم
-۸.۸	۹.۸	۱	متوسط
۴.۲	۹.۸	۱۴	زیاد
۱۳.۲	۹.۸	۲۳	خیلی زیاد
		۳۹	کل

جدول شماره ۱۲-آمارخی ۲ فرضیهٔ سوم

خی دو	۳۵.۵۶۴[a]
درجهٔ آزادی	۳
سطح معنی‌داری	.۰۰۰

همچنان که داده‌های جدول نشان می‌دهد، خی‌دوی محاسبه‌شده (۳۵.۵۶۴-) با درجهٔ آزادی df=3 معنی‌دار است. معنی‌داری خی‌دوی محاسبه‌شده به معنای تأیید فرض فرعی (۳) است. به عبارتی بین اقدامات تهاجمی در قالب هک مراکز حیاتی حریف، طراحی فریب سایبری و امنیت شبکهٔ اینترنت، رابطهٔ معناداری وجود دارد؛ بنابراین اجماع معناداری هر سه فرضیهٔ فرعی پژوهش، به معنای تأیید فرضیهٔ اصلی پژوهش است و می‌توان ادعا نمود که «ساختارهای امنیتی مؤثر در بهره‌برداری از شبکهٔ اینترنت، با سه لایهٔ راهکارهای پیشگیرانه، تدافعی و تهاجمی شکل می‌گیرد».

بحث و نتیجه‌گیری

بر اساس یافته‌های پژوهش، ترتیب توالی عمده‌ترین شیوه‌های مراقبت از ارتباطات در شبکهٔ اینترنت با استفاده از فنّاوری‌های واپایشی در قالب سطوح امنیتی که دارای هم‌پوشانی نسبت به یکدیگر هستند، بر اساس ساختار به‌هم‌پیوسته (پیرامون و شبکه و میزبان) بیان گردیده است، هم‌چنین برای بهره‌مندی از نظرات جامعهٔ خبرهٔ امنیتی و فنی، مهم‌ترین نکات یافته‌های پژوهش در معرض نظر آنان قرارگرفته و تقدم تأثیرگذاری راهکارهای مقابله با حملات و

تهدیدات شبکهٔ اینترنت مشخص گردید. سپس با روش علمی نیز اظهارات جامعهٔ خبره مورد تجزیه‌وتحلیل توصیفی و استنباطی قرارگرفت و فرضیه‌های پژوهشگران مورد تأیید واقع شده است؛ بنابراین شیوه‌های مدیریت فضای ارتباطی شبکهٔ اینترنت در شرایط امروزی، هنگامی از امنیت نسبی برخوردار است که هم‌زمان سه لایهٔ اقدامات امنیتی به ترتیب تقدم زیر را دربرداشته باشد.

۱- اقدامات پیشگیرانه با تأکید بر بهره‌برداری از نرم افزا و سخت‌افزار بومی، آینده‌پژوهی، مهارت کاربران، ساماندهی و تعادل.

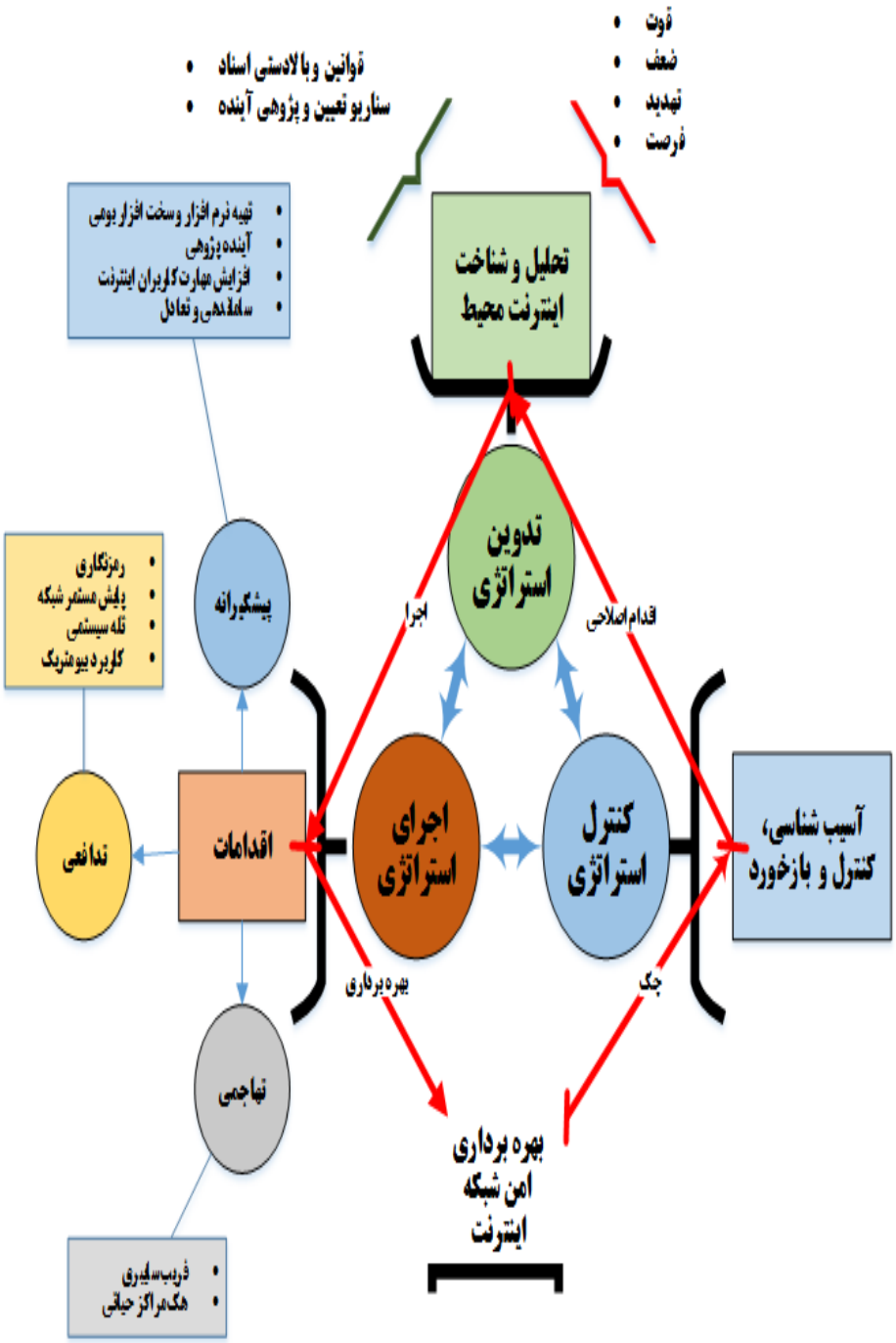
۲- اقدامات تدافعی با تأکید بر رمزنگاری، پایش مستمر شبکه، تلهٔ سامانه‌ای، کاربرد پایش زیست‌شناخت.

۳- اقدامات تهاجمی با تأکید بر طرح فریب سایبری، هک مراکز حیاتی.

بنابراین شرط مدیریت‌پذیر نمودن فضای اینترنتی برای ایجاد بستری امن، تلفیق و نظارت جدی بر این سه گزینه است که در ساختار امنیت شبکهٔ اینترنت بر مبنای نظریهٔ سامانه‌ای به شرح زیر ترسیم می‌گردد:

ابتدا اسناد فرادستی این ساختار در قالب‌بندهای قانون اساسی، تدابیر مقام معظم رهبری (مدظله‌العالی) و ابلاغیه‌های ستاد کل نیروهای مسلح مرتبط با موضوع -که تعیین‌کنندهٔ راهکارها و راهنمای طرح‌ریزی است- مشخص گردید. حلقهٔ ارتباط این بخش از ساختار با بخش‌های دیگر آن، طرح‌ریزی راهکارهاست که مدیران فنی سازمان با تکیه بر اسناد بالادستی اقدام به طراحی و برنامه‌ریزی و تقابل با تهدیدات شبکهٔ اینترنت می‌نمایند.

مطالبات تدوین‌شده در مرحلهٔ طرح‌ریزی امنیت شبکهٔ اینترنت، در چرخه و فرایند اجرایی قرارگرفته که شامل: تلفیق اقدامات پیشگیرانه؛ اقدامات تدافعی و اقدامات تهاجمی به‌طور تلفیقی به‌هم‌پیوسته بوده، سپس با واپایش و نظارت و بازخوردگیری نسبت به اصلاح مجدد فرایند و رسیدن به پیامد مطلوب استمرار می‌یابد.



شکل شماره ۵- ساختار امنیت کاربردی در بهره‌برداری از شبکهٔ اینترنت

منابع

۱. امام خامنه‌ای (مدظله‌العالی) (۱۳۸۸)؛ بیانات در دیدار با جمع کثیری از بسیجیان کشور.

۲. اخوان صفار، مصطفی؛ (۱۳۹۱)؛ «ارائه یک معماری جهت افزایش امنیت در آزمون‌های الکترونیکی با استفاده از روش‌های زیست‌شناخت چند عامله»، ***چهارمین کنفرانس برق و الکترونیک ایران*** ، دانشگاه آزاد اسلامی گناباد، ۹-۷ شهریور

۳. الوانی، مهدی و نصرا... میر شفیعی (۱۳۶۸)؛ ***مدیریت تولید***، مشهد ، شرکت به نشر.

۴. بوزان، باری (۱۳۷۸)؛ ***مردم، دولت‌ها و هراس***، ترجمه پژوهشکده مطالعات راهبردی، تهران: پژوهشکده مطالعات راهبردی

۵. پور وهاب، مهران؛ ابراهیمی آتانی، رضا (۱۳۹۳)؛ ***مجله علمی- پژوهشی پدافند الکترونیکی و سایبری و مجازی***، سال دوم، شماره ۴، زمستان

۶. تریف، تری و دیگران (۱۳۸۳)؛ ***مطالعات امنیتی نوین***، مترجمین علیرضا طیب، وحید بزرگی، تهران

۷. جلیلی، سعید و مهدی‌آبادی (۱۳۸۰)؛ مقاله نفوذ، راه‌های نفوذ به شبکه‌های رایانه‌ای و روش‌های تشخیص آن‌ها. ***اولین همایش اطلاع‌رسانی ن.م.***

۸. حافظ نیا؛ محمدرضا (۱۳۷۶)؛ جزوه کلاسی، دانشگاه عالی دفاع ملی،

۹. خزائی (۱۳۹۰)؛ مصاحبه ۱۲ شهریور، پایگاه آینده‌پژوهی.

۱۰. خلیلی پور رکن‌آبادی، علی؛ نورعلی وند، یاسر؛ تهدیدات سایبری و تأثیر آن بر امنیت ملی، ***فصلنامه مطالعات راهبردی شماره ۵۶***، شماره مسلسل

۱۱. روزنا، جیمز و دیگران (۱۳۹۰)؛ ***انقلاب اطلاعات، امنیت و فنّاوری‌های جدید***»، مترجم علیرضا طیب، تهران: پژوهشکده مطالعات راهبردی

۱۲. رئیسی وانانی، سارا؛ رئیسی وانانی، اسماعیل (۱۳۹۱)؛ راهکارهای امنیت شبکه، ***گاهنامه پژوهشی دانشگاه پیام نور استان چهارمحال و بختیاری***. شماره پنجم.

۱۳. شاه‌محمدی، محمد (۱۳۹۰)؛ مقاله جغرافیای سیاسی فنّاوری اطلاعات و ارتباطات، ***فصلنامه امنیت ملی*** دانشگاه عالی دفاع ملی، شماره ۱۵.

۱۴. شریفی محسن، رمضان زاده، مجتبی (۱۳۸۰)؛ بررسی امنیت در اطلاع‌رسانی، ***اولین همایش اطلاع‌رسانی ن.م.***

۱۵. قاسمی شبانکاره، کبرا؛ مختاری، وحید (۱۳۸۶)؛ امینی لاری، منصور؛ امنیت و تجارت الکترونیکی؛ ***چهارمین همایش ملی تجارت الکترونیک،۳ و ۴***.

۱۶. کلارک، یان (۱۳۸۶)؛ ***جهانی‌شدن و نظریه روابط بین‌الملل***، ترجمه فرامرز تقی لو، تهران : دفتر مطالعات سیاسی و بین‌المللی

۱۷. کلارک، یان (۱۳۸۶)؛ ***جهانی‌شدن و نظریه روابط بین‌الملل***، ترجمه فرامرز تقی لو، تهران: دفتر مطالعات سیاسی و بین‌المللی
۱۸. کبیری فر، فاطمه و صرافی زاده، اصغر؛ بررسی نقش اینترنت در توسعهٔ فرهنگی، ***مجله مدیریت فرهنگی***، سال چهارم شماره نهم مرکز آمار ایران
۱۹. محسنی، منوچهر (۱۳۸۰)؛ جامعه***شناسی جامعه اطلاعاتی***، تهران: نشر دیدار،
۲۰. مندل، رابرت (۱۳۷۹)؛ ***چهره متغیر امنیت ملی***، ترجمه پژوهشکده مطالعات راهبردی، تهران: پژوهشکده مطالعات راهبردی
۲۱. میرمحمدی، مهدی و محمدی لرد، عبدالمحمود (۱۳۸۷)؛ ***سیاست و اطلاعات***: مطالعه موردی ایالات‌متحده آمریکا، تهران: موسسه فرهنگی مطالعات و پژوهش‌های بین‌المللی ابرار معاصر تهران
۲۲. نای، جوزف (۱۳۸۷)؛ ***قدرت در عصر اطلاعات از واقع‌گرایی تا جهانی‌شدن***، ترجمه سعید میر ترابی، تهران :پژوهشکده مطالعات راهبردی.
۲۳. نوابخش، مهرداد و همکاران (۱۳۸۹)؛ بررسی آثار اینترنت و موبایل در تغییر هویت جوانان، ۲۳-۵ سال استان مازندران، ***مجله تخصصی جامعه‌شناسی مطالعات جوانان***
24. www.maghaleh.net/content-1032.html
25. http//www.ircert.com
26. http://iedco.ir/article/3/10
27. http://iedco.ir/article/3/10.
28. https://www.ircert.com/articles/Layered_Network_Security_5.htm
29. Lord, Kristin M. & Sharp, Travis (2011); "America's Cyber future Security and Prosperity in the Information Age", ***Center for a New American Security, Volume I***.
30. Nye, Joseph s. (2010); "***Cyber Power***", Belfer Center for Science and International Affairs
31. Theohary, Catherine A. & Rollins, Johan (2009); "***Cyber Security: Current Legislation, xecutive Branch Initiative, and Options for Congress***", Congressional Research Service.
32. Wolfers, Arnold (1962); ***Discord and Collaboration***, Baltimore: Johns Hopkins University Press
33. www.iransr.org.
34. www.monazam.ir
35. www.niazisoft.blogfa.com