راهبردهای دفاع سایبری در صنایع نفت، گاز و پتروشیمی

علی علیزاده اوصالو[1]، امیر علیزاده اوصالو[2]

۱- رئیس پدافند غیر عامل و مدیریت بحران پتروشیمی تبریز

تبریز، ایران

aaosalu@tpco.ir

۲- دانشگاه هوایی شهید ستاری

تهران، ایران

a.osalu@gmail.com

چکیده

امروزه تهدیدات سایبری پدیده‌ای غیرقابل انکار است که در حوزه‌ی امنیت ملی هر کشور، تعریف می‌شود. تهدیدات سایبری بر همه جنبه‌های جامعه از جمله تجارت و صنعت و روابط اجتماعی و سیاسی تأثیر می‌گذارد. دفاع غیر عامل به عنوان مکملِ دفاع عامل، اثربخش‌ترین روش دفاعی است که کاهش آسیب‌پذیری زیرساخت‌های ملی و مراکز حیاتی، حساس و مهم و پایداری ملی را بدنبال دارد. دفاع در برابر تهاجم سایبری علاوه بر دیدگاه پدافند عامل (مانند کارآمدی در برابر حملات سایبری، حفاظت از زیر ساخت‌های حیاتی و ...) می‌بایستی با رعایت الزامات پدافند غیر عامل انجام گیرد. صنعت نفت به عنوان حیاتی‌ترین شریان اقتصادی کشور، دارای کارکردهای سیاسی، اجتماعی و امنیتی فراوانی است که می‌تواند مورد تهاجم فیزیکی و مجازی قرار گیرد. واحدهای مختلف صنعت نفت با به کارگیری تجهیزات عمدتاً خارجی و سامانه‌های کنترلی کشورهای اروپایی (که کدنویسی، نحوه نفوذ و تخریب آن سامانه‌ها برای سازندگان آن‌ها کاملاً مشخص است) منبع بالقوه مناسبی برای تهدیدات سایبری به شمار می‌روند. اخیراً موضوع نفوذ ویروس استاکس نت در سامانه‌های کنترلی زیمنس در تأسیسات هسته‌ای، و نقش زیمنس در ارایه سامانه‌های کنترلی بسیاری از ادوات و تجهیزات صنعت نفت، نمونه بارزی از آسیب‌پذیری این صنعت در برابر تهدیدات سایبری دارد. در این مقاله با ارایه راهبردهای کلیدی دفاع در برابر حملات سایبری، تلاش می‌شود روش‌های آماده‌سازی برای مقابله با تهاجم سایبری در دستور کار مدیران این صنعت قرار گیرد.

کلمات کلیدی:

حوزه سایبر، تهدیدات سایبری، دفاع سایبری، پدافند غیر عامل، زیرساخت‌های حیاتی، صنعت نفت، گاز و پتروشیمی، سامانه‌های کنترل صنعتی، اتوماسیون صنعتی

۱- مقدمه

پدافند (دفاع) غیرعامل به عنوان مکملِ دفاع عامل، اثربخش‌ترین روش دفاعی است که موجب کاهش آسیب‌پذیری زیرساخت‌های ملی و مراکز حیاتی، حساس و مهم کشور در برابر تهدیدات می‌گردد. در قرن اخیر، فواصل جغرافیایی اهمیت سابق و جنگ افزارهای کلاسیک مفهوم خود را از دست داده‌اند. در قرن بیست و یکم، هیچ قدرتی به تنهایی نمی‌تواند سلطه خود را بر دیگران اعمال نماید بلکه یک اتحاد استراتژیک از مجموعه‌های قدرت است که منبع تهدید به شمار می‌رود. حوزه سایبر یکی از حوزه‌های بسیار حیاتی در فضای کنونی به شمار می‌رود. تهدیدات سایبری به عنوان پیامد حضور در فضای سایبری، بر همه جنبه‌های جامعه از جمله تجارت و صنعت و روابط اجتماعی و سیاسی تأثیر می‌گذارد. امروزه فناوری اطلاعات، زمان و هزینه تولیدات دفاعی را به شکل چشم‌گیری کاهش و کیفیت و انعطاف‌پذیری آن‌ها را افزایش داده است. تهدیدات این حوزه مانند حملات سایبری، می‌تواند دامنگیر بخش‌های مختلف کشور گردد. سرقت اطلاعات راهبردی، اقتصادی، نظامی و یا تخریب و از کاراندازی خدمات عمومی می‌تواند نمونه‌ای از نتایج جنگ سایبری باشد.

فضای سایبر در برگیرنده بخش اعظم محیط کارکردی دنیای مدرن خواهد بود و هرگونه تقابل نیروها در آن حوزه، پراهمیت تلقی می‌گردد. امروزه فاصله میان دنیای مجازی و دنیای واقعی به سرعت در حال کاهش است، که به نوبه خود می‌تواند، عاملی در جهت افزایش اهمیت هرگونه تقابل در فضای سایبر باشد. بر همین اساس اهداف اصلی حملات در حوزه سایبری می‌تواند شامل اهداف فنی و اهداف روانی باشد. در بخش فنی، اهداف اصلی حملات سایبری، شبکه‌های حیاتی هستند در صورت اخلال به مدت طولانی یا عملکرد نادرست، زندگی روزمره مردم و یا عملکرد عادی دستگاه‌های اجرایی کشور و مأموریت آن‌ها را مختل می‌کنند. شبکه حیاتی مورد نظر می‌تواند شبکه اینترنت، شبکه اورژانس، شبکه مالی، شبکه حمل و نقل، شبکه مخابرات، شبکه توزیع برق، شبکه تأمین آب، شبکه گازرسانی، شبکه فرماندهی و کنترل و یا هر شبکه دیگری که وابستگی عمده‌ای به ابزارهای رایانه‌ای داشته و از ساختار به هم متصل و یکپارچه برخوردار است باشد. اهداف روانی حملات سایبری نیز عمدتاً ناشی از موفقیت حمله بر علیه اهداف فنی بوده و به نوعی یک جنگ روانی محسوب می‌گردند. در این شرایط، مهاجمین، برتری فنی و موفقیت خود را به رخ کشیده و جایگاه خود را تثبیت می‌نمایند.

۲- تروریسم سایبری

واژه سایبر تروریسم، نخستین بار در دهه ۱۹۸۰ میلادی از سوی باری کالین (Barry Collin) وضع شد. سایبر تروریسم، حاصل تلاقی تروریسم و فضای مجازی است. سایبر تروریسم، بیشتر به معنای حمله یا تهدید به حمله علیه رایانه‌ها، شبکه‌های رایانه‌ای و اطلاعات ذخیره شده در آن‌هاست. از مهمترین دلایل تروریسم سایبری می‌توان به هزینه ناچیز این روش در برابر روش‌های تروریسمی سنتی، ناشناس ماندن، زیاد بودن تعداد و تنوع حملات، هدایت از راه دور بودن، سرمایه‌گذاری روانی کمتر و آموزش فیزیکی اندک و خطر مرگ کمتر اشاره نمود.

۳- سوابق حملات سایبری

در سال ۱۹۸۲ هکرهای طرفدار پاکستان تحت نام «باشگاه هکرهای پاکستانی» به کامپیوترهای هند حمله کردند. در سال ۱۹۹۹ تعداد این حملات به ۴۵ و در سال ۲۰۰۰ به ۱۳۳ مورد و در پایان اوت ۲۰۰۱ به ۲۵۷ مورد بالغ شد. همین گروه سایت وزارت دارایی و نیز نیروهای هوایی و دپارتمان انرژی آمریکا را مورد حمله قرار دادند.

هکرهای رژیم صهیونیستی هم با سیستم حمله DOS یا Denial Of Services در اکتبر ۲۰۰۰ به سایت‌های حماس و حزب الله حمله کردند. در مقابل هکرهای ضد رژیم صهیونیستی به سایت‌های اسراییلی حمله کرده و آن‌ها را با ترافیک قلابی درگیر کردند. از جمله سایت کنست (پارلمان اسراییل)، بانک‌ها، وزارت خارجه و وزارت دفاع اسرائیل مورد حملات سایبری متعدد قرار گرفت.

در سال ۱۹۹۹، مداخله ناتو در یوگسلاوی که به عملیات نیروهای متحد معروف شد، اولین کاربرد تمام عیار اجزاء جنگ اطلاعاتی در یک منازعه بود. در طول عملیات نیروهای متحد، هر دو طرف جنبه‌هایی از جنگ اطلاعاتی را برای صدمه زدن به دشمن بکار بردند. قسمت بیشتر این عملیات عبارت بود از کاربرد سنتی تبلیغات و ضد اطلاعات از طریق رسانه‌ها اما در عین حال تلاش‌هایی نیز برای مختل کردن ارتباطات طرف دیگر و راهبری اشکالی از جنگ الکترونیکی صورت گرفت. کاربرد فزاینده اینترنت در طول مناقشات به این منازعه صفت «اولین جنگ سایبری» یا «اولین جنگ

اینترنتی» را اعطا کرد. در این جنگ سرویس‌های اطلاعاتی از دو طرف ترافیک دیجیتالی طرف مقابل را زیر نظر داشتند.

در سال ۱۹۹۶ یک هکر رایانه‌ای مرتبط با جنبش برتری‌طلبی سفیدپوستان، ISP ماساچوست را به طور موقت از کار انداخت و به قسمتی از سیستم بایگانی ISP صدمه زد. در سال ۱۹۹۸، معترضان اسپانیایی، انستیتو جهانی ارتباطات (IGC) را با هزاران پیغام ایمیل قلابی مورد حمله قرار دادند. معترضان، صفحات وب را مسدود و تهدید کردند به تاکتیک‌های مشابهی علیه سازمان‌هایی که از خدمات این انستیتو استفاده کنند، اقدام خواهند کرد. اعتراض‌کنندگان می‌گفتند که IGC از تروریسم حمایت می‌کند؛ در سال ۱۹۹۸ چریک‌های تامیل، سفارتخانه‌های سریلانکا را با روزی ۸۰۰ ایمیل در یک دوره ۲ هفته‌ای، مورد حمله قرار دادند. مقامات امنیتی این مساله را به عنوان اولین حمله شناخته شده به وسیله تروریست‌ها علیه سیستم‌های رایانه‌ای دولت نام گذاشتند.

اخیراً شرکت صنایع سنگین میتسوبیشی، بزرگترین شرکت نظامی طرف قرارداد دولت ژاپن، مورد حمله هکرها قرار گرفته و به گفته یک روزنامه ژاپنی بخش پروژه‌های زیردریایی، موشک و ساخت نیروگاه‌های هسته‌ای این شرکت هدف اصلی حملات بوده‌اند. این شرکت سازنده صنایع دفاعی نظیر موشک‌های زمین به هوای پاتریوت و موشک‌های هوا به هوای AIM-7 Sparrow است. شرکت صنایع سنگین میتسوبیشی همچنین در پروژه ساخت هواپیمای Dreamliner ۷۸۷ بزرگترین همکار شرکت بوئینگ بوده‌است.

همچنین اخیراً شرکت Symantec (فعال در زمینه آنتی‌ویروس‌های رایانه‌ای) در زمینه مشاهده حملات سایبری جدید به شرکت‌های شیمیایی و دسترسی به اطلاعات فرایندی و طراحی آن شرکت‌ها، هشدار داده است. همچنین استفاده از ویروس استاکس نت برای نفوذ به سامانه کنترلی تأسیسات هسته‌ای کشورمان و انتشار ویروس جدید استارس از جدیدترین موارد حملات سایبری محسوب می‌شود.

شرکت امنیت سایبر سیمانتک می‌گوید حملات سایبری هدفمند در سال میلادی جدید بیش از پیش شرکت‌ها و سازمان‌ها را تهدید خواهند کرد.

در کل تعداد حملات سایبری بر پایه وب در سال ۲۰۱۰ نسبت به سال گذشته آن ۹۳ درصد افزایش داشت که یکی از دلایل افزایش آن استفاده هکرها از سیستم‌های کاهش طول آدرس‌های اینترنتی است. شرکت Symantec در گزارش سالانه خود می‌گوید هکرها با استفاده از سیستم‌های کاهش آدرس‌های اینترنتی، آدرس سایت‌های مخرب با کوتاه و خلاصه می‌کنند تا کمتر مورد شک کاربران قرار گیرد. این آدرس‌ها به وفور در هرزنامه‌های ارسالی در شبکه‌های اجتماعی یافت می‌شود.

در سال جدید روند رشد نفوذ هکرها با شبکه‌های اجتماعی افزایش خواهد یافت و با محبوب‌تر شدن آن‌ها، کاربران بیشتری قربانی حملات سایبری به شبکه‌های اجتماعی می‌شوند. به پیش‌بینی شرکت Symantec در سال جدید حملات به سیستم‌های پردازش قابل حمل از جمله گوشی‌های هوشمند و تبلت ۴۲ درصد افزایش می‌یابد. این شرکت می‌گوید اکنون تعداد کاربران این سیستم‌ها به اندازه‌ای رسیده‌است که بتواند هدف خوبی برای هکرها و مجرمان سایبری باشد.

چین بدون شک به عنوان بزرگترین اتاق فرمان حملات سایبری در جهان در نظر گرفته می‌شود. آمار حملات انجام شده که در آن‌ها نام چین به عنوان متهم اصلی مطرح بوده است همگان را به شگفتی وا داشته است. در زمانی که آمریکا و رژیم صهیونیستی توسط جوامع بین‌المللی عامل طراحی و انتشار بد افزار استاکس نت معرفی می‌شوند، کشور چین نیز به پی‌ریزی بسیاری از حملات عظیم سایبری علیه شرکت‌های معتبر آمریکایی و اروپایی و هم‌چنین شبکه‌های دولتی متهم می‌شود. به عنوان مثال، گفته می‌شود که چین عامل هک RSA's Secure ID database است که توانسته به رمزهای سری این شرکت و دستگاه‌هایش دسترسی داشته باشد. برطبق نظر تحلیل‌گران و محققین مربوطه در عملیات هک کردن این شرکت، از یک نوع تهدید مداوم پیشرفته (advanced persistent threat -APT) استفاده شده است که کشور چین در استفاده از این روش قدرتمند معروفیت جهانی دارد. از طرفی گفته می‌شود چین جهت اقدامات جاسوسی گسترده سرمایه‌گذاری عظیمی انجام داده است.

آر اس آ (RSA) تأیید کرد که نقص به وجود آمده در لاکهید مارتین (Lockheed Martin) در نتیجه‌ی اطلاعات هک شده و به دست آمده از بانک اطلاعاتی Secure ID بوده است. به علاوه حملات سایبری علیه نورث روپ گرومن (Northrop Grumman) نیز از نقص ایجاد شده در آر اس آ منشا می‌گیرد. هم‌چنین چینی‌ها متهم اصلی رخنه کردن به شبکه‌ی جهانی گوگل هستند. و نیز عامل حمله

سایبری به ۲۰ کمپانی بزرگ دیگر نیز در سال ۲۰۰۹ کشور چین بوده است. در ادامه‌ی حملات سایبری کشور چین می‌توان به حمله شدید سایبری انها به کمپانی نفت، گاز و انرژی نایت دراگون (Night Dragon) اشاره کرد. هکرهای چینی با به سرقت بردن اطلاعات مهم و امنیتی مربوط به مالکیت‌ها ضربه‌ی جبران نشدنی را به این شرکت مشهور وارد کردند. طبق تحقیق و بررسی محققان و دانشمندان در سراسر جهان، ارتش آزادی بخش خلق چین (PLA) در حال توسعه‌ی توانایی و امکانات جنگ سایبری پیشرفته است. این ارتش سایبری عظیم یک واحد یا گروه از مهاجم‌ها و هکرها را تشکیل داده است که علاوه بر افراد نظامی از افراد غیر نظامی و عادی نیز بهره می‌برد. هدف اصلی این گروه ایجاد تداخل و تخریب اهداف مشهور غربی است. به عنوان مثال مخابرات چین برای ۱۸ دقیقه در تاریخ ۸ آوریل ۲۰۱۰ ترافیک اینترنتی را از آمریکا و دیگر کشورها منحرف کرد. جالب است بدانید علاوه بر مطالب و نام شرکت‌های برده شده، چینی‌ها متهم یکه تاز هک شدن وب سایت‌های تجاری دل (Dell)، یاهوو (Yahoo) مایکروسافت (Microsoft) و آی بی ام (IBM) نیز هستند.

۴- امنیت‌سازی

رویکرد امنیت‌سازی عوامل متعددی را در کنار یک نظریه ساختار یافته مورد توجه قرار می‌دهد: با این وجود خود این رویکرد نیز نتیجه دو موضوع تئوریکی متفاوت است: اولی نئوپوزیتیویسم واقع‌گرای بوزان و پساپوزیتیویسم پسا ساختارگراویور.

با توجه به مکتب امنیتی کپنهاک، مشکلات تبدیل به مسائل امنیتی می‌شوند اما نه الزاماً به واسطه وجود یک تهدید واقعی، بلکه به این دلیل که مسئله مطرح، توسط عوامل کلیدی همانند یک تهدید بازنمایی و تثبیت می‌شود. مواضع انتقادی در مقابل مکتب گپنهاک از سوی متخصصان مکتب پاریس اتخاذ شده است. آن‌ها تنها بر رویه‌های گفتمانی متمرکز شده‌اند. با توجه به نظریات مکتب پاریس، فرایند امنیت‌سازی، متضمن بسیج گسترده‌ای از منابع برای حمایت از گفتمان غالب است. بالاترین درجه همبستگی چارچوب‌ها به عنوان الگوهای اجتماعی یک نتیجه واقعی برای امنیت‌سازی محسوب می‌شود.

۵- دفاع سایبری و پدافند غیر عامل

دفاع در برابر تهاجم سایبری علاوه بر دیدگاه پدافند عامل (مانند کارآمدی در برابر حملات سایبری، حفاظت از زیرساخت‌های حیاتی و ...) می‌بایستی با رعایت الزامات پدافند غیر عامل انجام گیرد. بر اساس دیدگاه پدافند غیر عامل، طراحی، بکارگیری و پیاده‌سازی سامانه‌های دفاع سایبری می‌بایستی با لحاظ نمودن الزاماتی در خصوص امنیت (security) و اطمینان‌پذیری بالا (reliability) باشد. عدم اختلال سامانه و عدم دسترسی افراد غیرمجاز به آن از دیگر الزامات پدافند غیرعامل سامانه‌های دفاع سایبری محسوب می‌شود.

۶- حوزه سایبر فرصت‌ها و تهدیدها

امروز عرصه سایبری پنجمین عرصه نبرد، پس از زمین، دریا، هوا و فضاست. در نبرد سایبری اساساً نوع نبرد، محتوایی نیست و رویکرد این نبرد، از دسترس خارج کردن سرویس‌ها و از کار انداختن ارایه دهندگان خدمات اینترنت و زیر ساخت‌هاست. این نوعی نبرد است. این نوع نبرد طبیعتاً لوازم خود را دارد؛ نیروی انسانی، سخت‌افزار، نرم‌افزار و جنگ‌افزاری متمایز از دیگر جنگ‌ها. با توجه به ورود فضای سایبر به تمامی عرصه‌های زندگی افراد از موضوعات علمی گرفته تا کار، سرگرمی، اقتصاد، آموزش و ارتباطات، مهاجمین می‌توانند در کار عمومی و روزمره مردم جامعه هدف، اختلال ایجاد کند. افزون بر این چون بسیاری از ارتباطات میان یا درون سازمانی هم‌اکنون بر بستر اینترنت شکل گرفته است، از کار انداختن سرویس اینترنت خود می‌تواند زمینه‌ساز آشوب و نا آرامی در کشورها گردد

سال ۲۰۰۹ حوزه فرماندهی سایبری ارتش آمریکا با مأموریت مشخص حمله و دفاع در عرصه سایبری راه‌اندازی شد. قوانین جدیدی هم در حوزه‌ی حملات و دفاع سایبری در سطح جهان در حال مصوب شدن است تا حملات سایبری در گروه حملات با سلاح‌های کشتار جمعی و هسته‌ای قرار گیرد.

مؤسسه‌ی دیفنس تک از مؤسسه‌های نظامی و امنیتی ایالات متحده‌ی آمریکا، اقدام به انتشار مقاله‌ای با عنوان «ارزیابی ارتش سایبری ایران» نمود. در این مقاله ارتش سایبری ایران زیر مجموعه‌ای از سپاه پاسداران انقلاب اسلامی معرفی شده است. این مؤسسه با توجه به آمار دریافتی از سازمان اطلاعات آمریکا (CIA)، ایران را جزء پنج کشور دارای قوی‌ترین نیروی سایبری معرفی کرده

و تعداد نیروهای سایبری سپاه را ۲۴۰۰ نفر به اضافه ۱۲۰۰۰ نفر نیروی ذخیره و بودجه‌ی این مجموعه از سپاه را ۷۶ میلیون دلار برآورد کرده است. به تازگی نیز روزنامه‌ی «تریبون» چاپ فرانسه، ارتش سایبری ایران را ۲۵۰ هزار نفر تخمین زده است.

بنابراین حوزه سایبری در حال سازماندهی نیروی متخصصی برای فعالیت در سطوح بالای تکنولوژی بوده و این موضوع از نظر اجتماعی و اقتصادی می‌تواند یک فرصت محسوب شود. با این حال بکارگیری نیروی متخصصان این حوزه در طرح‌ریزی حملات جدیدتر و غیرقابل کنترل‌تر یک تهدید بالقوه در این زمینه به شمار می‌رود.

برای ایجاد یک مجموعه هماهنگ و یکپارچه از استراتژی‌های امنیت در فضای سایبری در سطوح ملی، منطقه‌ای و بین‌المللی باید موارد زیر مد نظر قرار گیرند:

- مشارکت بخش‌های عمومی و خصوصی
- آگاهی بخشی عمومی
- استفاده از تجربیات، راهبردها و استانداردهای بین‌المللی
- اشتراک اطلاعات بخش خصوصی با مراکز دولتی
- آموزش نیروی انسانی
- رعایت اهمیت حریم خصوصی
- ارزیابی آسیب‌پذیری، هشدار و عکس‌العمل با برگزاری رزمایش‌ها
- همکاری بین‌المللی در زمینه امنیت فضای سایبری
- وضع قوانین حوزه سایبری

۷- نقش نیروی انسانی در حوزه دفاع سایبری

برای مقابله با چالش سرمایه انسانی کار آمد از لحاظ امنیت در فضای سایبری داشتن افرادی با مهارت در موضوع‌های فنی و استفاده از عناصر راهبردی زیر، کمک خواهد کرد تا امنیت اینگونه محیط‌ها افزایش یابد:

- ✓ ترویج و توسعه برنامه‌های آموزشی دقیق در راستای تعلیم نیروی انسانی کارآمد در مراکز آموزشی از جمله مدارس.
- ✓ حمایت از توسعه و تصویب گواهی نامه‌های حرفه‌ای که از لحاظ فنی بسیار دقیق و شامل مؤلفه‌های عملی آموزشی و نظارتی سخت باشند.
- ✓ استفاده از فرایند ترکیبی استخدام و فرآیند کسب و منابع آموزشی به منظور بالا بردن صلاحیت فنی کسانی که از سیستم‌های دولتی حفاظت ویا با آن‌ها کار می‌کنند.
- ✓ اطمینان از وجود مسیر شغلی مناسب برای حفظ افراد با مهارت فنی سطح بالا

۸- راهبردهای عمومی دفاع از فضای سایبری

در راستای دفاع از فضای سایبری، اقدامات راهبردی زیر، می‌بایستی در اولویت کاری دستگاه‌های قانون گذاری و اجرایی کشور قرار گیرد:

- ➢ شناسایی فضای سایبری به عنوان یک حوزه جدید ملی (در کنار دیگر حوزه‌ها مانند زمین، هوا و دریا) که دفاع از آن جزء اولویت‌های ویژه می‌باشد.
- ➢ تأسیس فرماندهی مرکزی برای دفاع از فضای سایبری در سطح ملی (هم‌اکنون با تأسیس پایگاه پدافند دفاع سایبری اجرایی شده است).
- ➢ مدنظر قرار دادن توسعه زیرساخت‌های مهم و حیاتی و سامانه‌های امنیتی به عنوان اولویت اصلی، ضمن دفاع از سایر بخش‌ها؛ از جمله دفاع از اطلاعات موجود در دانشگاه‌ها و مراکز تحقیقاتی و دفاع از شرکت‌هایی که بر اقتصاد کشور تأثیرگذارند، لیکن جزء زیرساخت‌های دولتی طبقه‌بندی نشده‌اند.
- ➢ ایجاد سامانه دفاع همه‌جانبه و پویا در فضای سایبری نظیر سامانه‌ای که توسط وزارت دفاع ایالات متحده ایجاد شده است.
- ➢ همکاری پایدار در حوزه سایبری میان بخش دولتی، بخش امنیتی و بخش خصوصی.
- ➢ همکاری در ارتباط با موضوع فضای سایبری با کشورهای خارجی، بویژه کشورهای متحد.
- ➢ تصویب قانونی ویژه راجع به فضای سایبری و اطمینان از اجرای صحیح این قانون.
- ➢ کمک به عموم مردم در راستای افزایش آگاهی آن‌ها از فضای سایبری، توسعه قابلیت‌های دفاع عمومی در این حوزه و ارائه مشوق‌های لازم به شرکت‌ها و افراد به منظور دست‌یابی به نرم‌افزارهای دفاعی و در عین حال افزایش

نظارت و کنترل بر شرکت‌هایی که در زمینه بهینه‌سازی چنین نرم‌افزارهایی کار می‌کنند.

- استفاده از پیشرفته‌ترین و به روزترین پشتیبانی‌ها و ابزارآلات فنی مرتبط با فضای سایبری.

۹- راهبردهای دفاع سایبری در صنایع نفت، گاز و پتروشیمی

استفاده از بدافزارهای (malwares) آسیب‌رسان به بانک‌ها و سایت‌های اطلاعاتی و تأسیسات صنعتی و زیرساخت‌های کشورها نوعی پیشروی در جنگ نرم به شمار می‌رود.

اخلال سامانه‌های سایبری کشورهای هدف و دسترسی به منابع اطلاعاتی آن‌ها و ضربه زدن به روند فعالیت‌های مختلف کشورها از جمله فعالیت‌های امنیتی، نظامی، دفاعی، حوزه‌های مالی، بهداشت عمومی یا فعالیت‌های هسته‌ای، هدفی است که در قالب‌های مختلف در حال پیگیری و اجراست. مقابله با این روند پیچیده، نیازمند هوشیاری، شناخت و آماده‌باش همیشگی است.

همان‌طور که افکار عمومی باید نسبت به دلایل و ظرایف آمادگی دفاعی کشور توجیه بوده و دارای اطلاعات کافی باشد تا حامی و مشوق پاسداری از کشور و ارزش‌های موجود در آن باشد، مردم و افکار عمومی باید هرچه بیشتر نسبت به پاسداری از فضای سایبری که اهمیت آن کمتر از دیگر فضاها و حریم‌ها نیست، هرچه بیشتر توجیه و آگاه باشند.

اگر آمادگی مقابله با حملات سایبری وجود نداشته باشد و حملات با موفقیت همراه شود، امکان خطای صنعتی در زیرساخت‌های پالایشگاهی و صنعتی زیاد بوده و احتمال وقوع حوادث ناگواری وجود دارد.

به عنوان مثال اختلال در یک مجتمع پتروشیمی ممکن است به آتش‌سوزی و آلودگی شیمیایی خطرناک برای مردم و محیط‌زیست مانند حادثه بوپال هند منجر شود. در صورت اختلال در حوزه نفت، گاز، برق و پتروشیمی امکان دارد خسارت‌های سنگین به تأسیسات وارد شود.

سامانه‌های کنترلی در صنایع نفت و گاز برای انتقال داده و فرامین از اتاق‌های کنترل به واحدهای عملیاتی مورد استفاده قرار می‌گیرد. همچنین تجزیه و تحلیل داده‌ها نیز در پردازشگرهای الکترونیکی انجام گرفته و کل عملیات واحد در آن سامانه راهبری می‌شود.

اولین قدم‌های اتوماسیون صنعتی در حدود چهل سال قبل و ارایه سامانه‌های کنترلی PLC آغاز گردید. این سامانه به عنوان کنترلرهای منطقی برنامه‌ریزی شده (Programming Logic Controllers) عمل تحلیل داده و انتقال فرامین و اجرای دستورات را با استفاده از نیروی الکتریکی و یا نیروی فشار هوا (pneumatic) انجام می‌دادند.

با پیشرفت علمِ کنترل و اتوماسیون صنعتی، سامانه‌های (DCS) رایج شدند. این سامانه کنترلی توزیع یافته (Distributed Control Systems) با دقت و انعطاف‌پذیری بالا، قابلیت فراوانی برای توسعه اتوماسیون صنعتی در عملیات پیچیده فراهم نمودند.

طی سالیان اخیر استفاده از ادوات هوشمند (Smart Equipment) و سامانه‌های کنترلی جدید (مانند Fieldbus و ...) باعث پیچیدگی بیشتر سامانه‌های کنترلی و دقت بسیار بالای آن‌ها در کنترل فرآیندها گردیده است.

تمامی این سامانه‌های کنترلی از پردازشگرهای عمدتاً اروپایی و آمریکایی استفاده می‌نمایند که به عنوان پاشنه آشیل تمامی سامانه‌های کنترلی محسوب می‌شوند. علاوه بر جنبه‌های اقتصادی خرید این سامانه‌ها و مشکلات ناشی از تحریم و اختلال در ارایه خدمات فنی و مهندسی به شرکت‌های ایرانی، زمینه نفوذ در زیر ساخت‌های حیاتی این صنعت عظیم را فراهم نموده است. عمده‌ترین حملات سایبری با هدف اختلال در عملکرد سامانه‌های کنترلی صورت گرفته و موجب خسارت اقتصادی، سیاسی و چه بسا انسانی فراوانی خواهد شد.

راهکارهای اولیه دفاع در برابر حملات سایبری را می‌توان در ۳ شاخه اصلی آموزش، ساز و کار حقوقی و تقویت دفاعی طبقه‌بندی کرد.

۹-۱- آموزش

مهم‌ترین مرحله در جلوگیری از حملات سایبری آموزش عمومی به مردم و مسئولین سیاسی و امنیتی است. در خصوص آموزش عمومی، مهم‌ترین نکته این است که کاربران اینترنت را نسبت به ایمن‌تر کردن رایانه‌های شخصی متقاعد کرد و در این راه می‌توان از آموزش‌های رسمی و اطلاع‌رسانی از طریق رسانه‌های عمومی بهره گرفت. آموزش و اطلاع‌رسانی به مقامات ارشد سیاسی و امنیتی نیز جایگاه ویژه‌ای دارد و باید این مقامات نسبت به حساسیت مسأله مطلع شوند تا تمهیدات لازم را برای مقابله با سایبرتروریسم عملی کنند.

۹-۲- ساز و کار حقوقی

مرحله بعد در مبارزه با سایبرتروریسم، استفاده از ساز و کار حقوقی و قضایی مناسب است. اولین گام در این راه تدوین و یک شکل کردن قوانین جرایم رایانه‌ای و اینترنتی خواهد بود. وجود خلاءهای قانونی، نیروهای امنیتی را در مقابله با جرایم رایانه‌ای و اینترنتی، سردرگم می‌کند و توانایی واکنش به موقع و مناسب را از آنان می‌گیرد.

ایجاد دادگاه‌های خاص ملی و بین‌المللی جرایم رایانه‌ای و اینترنتی نیز از جمله گام‌های بسیار مهم و مؤثر در مقابله با حملات سایبری است. وجود این دادگاه‌های خاص، رسیدگی به این جرایم را آسان‌تر و سریع‌تر می‌کند و در نتیجه مجرمان یقین خواهند داشت که بسرعت و به طور ویژه‌ای به جرم آن‌ها رسیدگی خواهد شد و این موضوع گامی بزرگ در خصوص مبارزه با حملات سایبری محسوب می‌شود.

۹-۳- تقویت دفاعی

ایجاد سازمان‌های مسؤل مقابله با حملات سایبری، مهم‌ترین راهکار دفاعی در برابر حملات سایبری خواهد بود. لازم است سازمان‌های امنیتی خاصی تأسیس شوند که مسؤلیت آن‌ها مطالعه و تحقیق و مقابله با حملات سایبر باشد. این سازمان‌ها می‌توانند درون نهادهای مختلف امنیتی و سیاسی شکل گیرد؛ ولی مسأله مهم این است که حوزه کاری هر کدام از آن‌ها باید به طور دقیق مشخص باشد و مبادله اطلاعات سازمان‌های امنیتی مختلف مد نظر قرار گیرد.

در صنعت و در حوزه فناوری اطلاعات، زیرساخت شبکه‌های الکترونیکی، سوئیچ‌های مخابراتی و مراکز داده به عنوان یکی از اهداف اصلی در لحظات اولیه تهاجم در جنگ‌های اخیر مورد توجه ویژه قرار داشته است، لذا بایستی در طراحی، مهندسی، اجرا و بکارگیری آن‌ها را در تمامی سطوح مدیریتی، هوشمندانه عمل نمود. امروزه فناوری اطلاعات در مأموریت تمامی دستگاه‌های اجرایی کشور حتی کوچکترین عملکردهای اجرایی، قابلیت‌های ممتازی را به وجود آورده است، در حالی که اگر این توسعه با مشاوره امنیتی مناسب و رویکرد صحیح از شناخت تهدیدات تخصصی آن حوزه نباشد در زمان بحران و شرایط اضطرار، انتظارات لازم برای استفاده از فناوری در بالابردن توان مدیریت را برآورده نمی‌نماید. در زمان بحران، فناوری جدید بدلیل عدم عملکرد صحیح، شرایط پیچیده‌ای از بحران را رقم خواهد زد که در حوزه مدیریت بحران از آن تحت عنوان هم‌افزایی بحران‌ها و تبدیل یک بحران کوچک به بحران منطقه‌ای یا ملی یاد می‌کنند.

۹-۴- راهبردهای دفاع سایبری برای زیرساخت‌های حیاتی در صنعت نفت

راهبردهای کاهش مخاطرات زیر ساخت‌های حیاتی در صنعت نفت در برابر حملات سایبری به شرح ذیل می‌باشد:

- دارا بودن سامانه‌ها و شبکه‌های هشدار دهنده شرایط اضطراری برای تهدیدات سایبری
- ارتقاء سطح دانش و آگاهی کارکنان تا به درک افراد از ماهیت و وسعت زیر ساخت اطلاعات حساس خود کمک گردد.
- تقویت مشارکت میان بخش عمومی و بخش خصوصی و تجزیه و تحلیل اطلاعات زیرساخت‌های خود به کمک متخصصین این حوزه
- رعیات امنیت داده‌های زیر ساخت‌های حیاتی ضمن در دسترس بودن داده‌ها برای افراد مرتبط
- وضع قوانین و رویه‌های مناسب برای مقابله با مشکلات امنیتی
- برگزاری رزمایش و تمرین برای سنجش آمادگی در برابر تهدیدات سایبری

۱۰- بحث و نتیجه‌گیری

شناسایی حوزه سایبری به عنوان حوزه جدید راهبردی و ضرورت دفاع از آن ضرورتی انکارناپذیر است. صنایع نفت، گاز و پتروشیمی با دارا بودن جایگاه راهبردی در امنیت اقتصادی، سیاسی کشور می‌بایستی با تمامی امکانات در دسترس مورد حفاظت قرار گیرند. حفاظت از تجهیزات و تأسیسات صنعت نفت بدون توجه ویژه به حفاظت سایبری این صنعت عظیم امکان‌پذیر نمی‌باشد. واحدهای مختلف صنعت نفت با به کارگیری تجهیزات عمدتاً خارجی و سامانه‌های کنترلی کشورهای اروپایی (که کدنویسی، نحوه نفوذ و تخریب آن سامانه‌ها برای سازندگان آن‌ها کاملاً مشخص است) منبع بالقوه مناسبی برای تهدیدات سایبری به شمار می‌روند. اتخاذ راهبردهای دفاعی مناسب جزو اولویت‌های حفاظتی از این صنعت عظیم ملی محسوب می‌شود که می‌بایستی مورد توجه ویژه قرار

گیرد. در این مقاله سعی گردید راهبردهای عمومی دفاع از فضای سایبری و راهبردهای تخصصی دفاع سایبری با کاربرد ویژه در صنعت نفت ارایه شده و اولویت‌های دفاع در برابر حملات سایبری در این حوزه مورد بررسی قرار گیرد.

مراجع

۱. علیزاده اوصالو، محمد حسین مهدی غلامی و سیاوش درفشی " نقش سامانه‌های اطلاعاتی و برنامه‌ریزی در مدیریت بحرانها "، دومین کنفرانس بین المللی جایگاه HSE در سازمانها، تهران، ۱۳۸۸

۲. جک گاتز چاک؛ مدیریت بحران (در بخش‌های خصوصی و دولتی)؛ ترجمهٔ علی پارسائیان؛ انتشارات ترمه؛ چاپ اول، تهران؛ ۱۳۸۳؛ ص ۳۰.

۳. علیزاده اوصالو، محمد حسین مهدی غلامی و سیاوش درفشی " به روز رسانی سامانه بهداشت و درمان صنعت نفت در مواقع بروز شرایط اضطراری"، اولین کنفرانس مدیریت جامع بحران و حوادث غیر مترقبه، تهران، ۱۳۸۶

4. Mitroff, Ian I.; Paul Shrivastava; and Ferdaus E. Udwadia; “Effective 2. Crisis Management”; Academy of Management Executive Journal; 1978; Vol. 1; P .60.

5. Booth, Simon; “Crisis Management Strategy”; Routledge; 1993; P. 64.

۶. راهنمای مدیریت در برابر شرایط اضطراری در سیستم های مدیریت بهداشت، ایمنی و محیط زیست، شرکت ملی صنایع پتروشیمی

۷. روش اجرایی مدیریت بحران در شرکت ملی صنایع پتروشیمی

8. http://www.nipc.net/

9. http://www.abanet.org/abapubs/books/cybercrime

10. http://cybersecuritycooperation.org/documents

11. Garfinkel, Simson, Gene Spafford, and Alan Schwartz. “Practical Unix and Internet Security”, 3rd Edition. Cambridge,Ma:OReilly and Associates,Inc. 2009

12. George Sadowsky, James X., Alan Greenberg, and Alan Schwartz. “Information Technology Security”, info Dev, world bank, 2010.