



تحلیل لایه های امنیت سایبری در زیر ساخت های ماهواره ای و تحول تهدیدات هوافضائی

نویسنده اول: مهدی طاهری

کارشناسی مدیریت دفاعی دانشگاه افسری امام علی (ع)، تهران، ایران.

taheritmehdi@gmail.com

نویسنده دوم: رضا اژدری

کارشناسی فرماندهی و کنترل دانشگاه افسری پدافند هوایی خاتم الانبیاء (ص)، تهران، ایران.

Reza.azhdarii84@gmail.com

نویسنده سوم: امیر مهدی لزگی

کارشناسی مهندسی برق، دانشگاه افسری پدافند هوایی خاتم الانبیاء (ص)، تهران، ایران.

amirmahdilezgi@gmail.com

چکیده

بخش ارتباطات ماهواره ای (satcoms) نمونه بارزی از یک سیستم پیچیده سایبری-فیزیکی هوافضا است. برای ارائه قابلیت ارتباطی امن و قوی، سیستم های satcoms به گونه ای طراحی شده اند که دفاع عمیقی را در برابر حملات هدفمند و خرابی قطعات پیاده سازی کنند و همچنین در شرایط سخت محیطی به طور مؤثر عمل کنند. با توجه به هزینه گزاف جایگزینی، فضاپیماهای satcoms اغلب با طول عمر بیش از یک دهه طراحی می شوند و باید خدمات مداومی ارائه دهند - جایی که هرگونه خرابی غیرقابل قبول تلقی می شود.

اخیراً، چندین دولت بین المللی استراتژی های سایبری را توسعه داده اند که برخلاف روش سنتی «قرنطینه، حل و فصل، اصلاح» است. به عنوان مثال، دولت ایالات متحده اکنون تداوم قابلیت های عملیاتی را به عنوان یک اولویت - فراتر از جداسازی و قرنطینه سیستم هایی که ممکن است در یک حمله سایبری تحت تأثیر قرار گیرند - الزامی می داند. این رویکرد جدید نه تنها به سطوح مختلف افزونگی و یک رویکرد ساختاریافته برای دفاع سایبری نیاز دارد، بلکه به مسیرهای اطلاعاتی و خدماتی متعددی نیاز دارد که از پروتکل های مستقل و مسیرهای فروشندگان برای ارائه قابلیت های عملیاتی مداوم استفاده می کنند.

در این مقاله، ما روشی را ارائه می دهیم که از رویه های هوافضا اقتباس شده است و طراحی سیستم هایی را که برای ارائه تداوم خدمات حتی در هنگام حمله طراحی شده اند، تسهیل می کند. ما همچنین از بهترین شیوه های تثبیت شده در فضای امنیت سایبری استفاده می کنیم و بهبودهایی را برای روش های رایج موجود در صنعت هوافضا پیشنهاد می دهیم.

واژگان کلیدی: امنیت سایبری هوافضایی، سیستم سایبری-فیزیکی هوافضایی، دفاع در عمق فضایی، چرخه عمر امن SATCOM، زیر ساخت مخابرات ماهواره ای و آموزش امنیت فناوری اطلاعات برای فضای سایبری.

مقدمه

با پیشرفت در عصر اطلاعات، به طور فزاینده ای از تهدیدی که تروریست های سایبری برای شبکه های دولتی و نظامی ایالات متحده در سراسر جهان ایجاد می کنند، آگاه می شویم. در گذشته، فناوری اطلاعات برای دولت چیزی بیش از کمک به دفاتر دولتی در وظایف اداری نبود، اما اکنون به بخش مهمی از عملیات نظامی در سطح جهان تبدیل شده است. زیرساخت فضای مجازی ارتش



ایالات متحده از ده‌ها هزار شبکه و میلیون‌ها دستگاه محاسباتی تشکیل شده است که بسیاری از آنها در سطح بین‌المللی قرار دارند. ۱. نیروهای ما باید برای رویارویی با دشمنان همیشه مهاجم در این حوزه جنگی جدید آماده باشند. توجه جامعه بین‌المللی به این نکته جلب شده است که رویکرد پیشگیرانه برای محافظت از دارایی‌های سایبری ضروری است و بسیاری از کشورها اسناد استراتژی سایبری را که در دسترس عموم قرار دارد، منتشر کرده‌اند که رویکرد آنها به دفاع سایبری را تشریح می‌کند. ۲. دستور اجرایی ۱۳۶۳۶ ایالات متحده در فوریه ۲۰۱۳ توسط رئیس‌جمهور باراک اوباما صادر شد که به لزوم "بهبود امنیت سایبری زیرساخت‌های حیاتی" پرداخت و بر لزوم اتخاذ یک چارچوب مشارکتی و انگیزشی در نهادهای دولتی و تجاری تأکید کرد، با این درک که ما به شدت برای تهدیداتی که حملات سایبری برای ایالات متحده آمریکا ایجاد می‌کند، آماده نیستیم. ۳. این چارچوب در فوریه ۲۰۱۴ منتشر شد و توسعه سیاست‌ها و رویه‌هایی را تشویق می‌کند که در هسته خود، برای شناسایی، محافظت، تشخیص، پاسخ و بازایی از حملات سایبری ساخته شده‌اند. اگرچه این چارچوب به آنچه باید انجام شود می‌پردازد، اما تکنیک‌ها یا فناوری‌هایی را که باید برای تحقق پتانسیل آن پیاده‌سازی شوند، مشخص نمی‌کند. ما باید در مورد چگونگی رویکرد بهتر به دفاع سایبری برای حفظ امنیت ملی بحث کنیم. نگاهی تازه به شیوه‌های امنیت سایبری هنگام ارزیابی حملات اخیر که علیه شرکت‌های بزرگ رخ داده است، ضروری است. در گذشته، پاسخ به یک نقض امنیتی اغلب شامل جداسازی سیستم آسیب‌دیده بود که سپس قبل از بازگرداندن آن به چرخه تولید، پاکسازی، بازسازی یا به هر طریق دیگری بازایی می‌شد. در این میان، یک سیستم پشتیبان یا افزونه، بار سیستم آسیب‌دیده را بر عهده می‌گرفت. این راه‌حل رایج ممکن است با حرکت به سوی آینده، دیگر یک روش پاسخ به حادثه کافی نباشد. در دسامبر ۲۰۱۴، سونی پیکچرز انترتینمنت (SPE) توسط یک گروه هکری که خود را «نگهبانان صلح» معرفی می‌کردند، مورد حمله قرار گرفت. اداره تحقیقات فدرال (FBI) تأیید کرد که این سازمان با دولت کره شمالی مرتبط است. با توجه به این حمله و سایر حملات تحت حمایت دولت که در چند سال گذشته رخ داده است، می‌توانیم پیش‌بینی کنیم که جنگ سایبری تحت هدایت دولت در آینده نزدیک محتمل است. با توجه به ماهیت حمله سونی، می‌توانیم ببینیم که چگونه رویکرد «قرنطینه، حل و فصل، اصلاح» برای بازایی از حملات سایبری بی‌اثر خواهد بود. طبق بیانیه مطبوعاتی FBI در ۱۹ دسامبر ۲۰۱۴، نه تنها مقدار زیادی از داده‌های حساس از SPE به سرقت رفت، بلکه «این حملات همچنین هزاران رایانه SPE را از کار انداخت، SPE را مجبور کرد کل شبکه رایانه‌ای خود را آفلاین کند و عملیات تجاری شرکت را به طور قابل توجهی مختل کرد.» ۵ مهاجمان ثابت کرده‌اند که توانایی انجام عملیات در مقیاس بزرگ علیه اهداف مهم را دارند. با این قابلیت‌ها، نمی‌توان فرض کرد که طرحی برای قرنطینه کردن سیستم‌های آسیب‌دیده پس از حمله سایبری و در عین حال حفظ دسترسی به سرویس، یک روش

بازیابی احتمالی در آینده باشد. ما باید راههایی برای به حداکثر رساندن دسترسی به سرویس‌ها حتی در بحبوحه یک حمله سایبری پیدا کنیم.

این درک که ما به یک استراتژی سایبری قوی‌تر با تأکید بر به حداکثر رساندن دسترسی نیاز داریم، چیز جدیدی نیست. در سال ۲۰۱۰، ژنرال چارلز شوگ، معاون فرمانده واحد ۲۴ نیروی هوایی، اظهار داشت: «ما می‌خواهیم مطمئن شویم که فضای سایبری از ابتدا در فرآیند برنامه‌ریزی عملیاتی ادغام شده است. ما باید یاد بگیریم که چگونه از طریق حملات سایبری مبارزه کنیم.» ۶ با توجه به این الزام برای حفظ تداوم خدمات در بحبوحه حملات سایبری، تلاش‌هایی برای اتخاذ شیوه‌های جدیدی انجام می‌شود که به ما امکان انعطاف‌پذیری لازم برای دستیابی به این هدف را می‌دهد.

با این حال، در جستجوی بهترین شیوه‌های امنیت سایبری برای دسترسی‌پذیری، نیازی به اختراع مجدد چرخ نداریم. در بخش‌های بعدی، در مورد چگونگی یادگیری درس‌های مؤثر از صنعت ارتباطات ماهواره‌ای که دهه‌هاست با چنین الزاماتی روبرو بوده است، بحث خواهیم کرد.

با به کارگیری شیوه‌های اتخاذ شده توسط صنعت هوافضا، روشی را برای استراتژیست‌های سایبری و معماران سیستم توسعه خواهیم داد تا دسترسی‌پذیری را بر حفاظت از اطلاعات اولویت دهند و در نهایت در دستیابی به هر دو مؤثرتر باشند. هدف ما این است که با در نظر گرفتن طراحی ماهواره و مکانیسم‌های دفاعی، فراتر از چارچوب شیوه‌های فعلی امنیت سایبری فکر کنیم. اینها به استراتژی دفاع سایبری ما کمک می‌کنند تا بتوانیم در پیاده‌سازی یک روش جدید امنیت سایبری مؤثرتر عمل کنیم. ماهواره‌ها به عنوان یک سیستم سایبری-فیزیکی

فناوری ارتباطات ماهواره‌ای (SatCom) تقریباً به اندازه محاسبات الکترونیکی وجود داشته است. این سیستم‌های پیچیده سایبری-فیزیکی، رایج‌ترین دستگاه‌های شبکه در حوزه فناوری اطلاعات (IT) نیستند، اما مانند سایر سیستم‌های فناوری اطلاعات، طی دهه‌های متمادی تکامل یافته و سازگار شده‌اند. صنعت هوافضا مجبور بوده است روش‌های امن و قوی برای محافظت از منابع خود در برابر آسیب‌های فیزیکی و همچنین حملات سایبری ایجاد کند. به دلیل عدم توانایی در انجام تعمیر و نگهداری سخت‌افزار در ماهواره‌های مستقر، طراحی و پیاده‌سازی سیستم‌های قوی، کلید حفظ دسترسی و تداوم خدمات است. از این میراث طراحی ماهواره است که می‌توانیم استراتژی‌هایی را برای استفاده در سایر سیستم‌های سایبری کشف و پیاده‌سازی کنیم.

با این حال، باید درک کرد که بخش زیادی از زیرساخت سیستم‌های ماهواره‌ای ما در حال ادغام در ستون فقرات اینترنت و برقراری ارتباط با استفاده از پروتکل‌های آشنا برای متخصصان فناوری اطلاعات است. اکنون ما خدمات تلویزیونی، تلفنی، GPS و اینترنتی را از طریق لینک‌های ماهواره‌ای ارائه می‌دهیم. علاوه بر این، ایستگاه‌های زمینی که برای انتقال سیگنال‌های ماهواره‌ای به مقاصد مناسب خود بسیار مهم هستند نیز به اینترنت متصل هستند. این ادغام فناوری‌ها، شبکه‌های ماهواره‌ای را به شبکه جهانی وسیع‌تری از سیستم‌ها سوق می‌دهد که آنها را در معرض خطر حمله از سوی نهادهای خارجی قرار می‌دهد. مگر اینکه متخصصان امنیت سایبری مایل به پذیرش مسئولیت ادغام این شبکه‌ها در ارزیابی‌های ریسک امنیت سایبری خود باشند، لینک‌های ماهواره‌ای ممکن است به یک نقطه ضعف بزرگ در توانایی ما برای جلوگیری از حملات سایبری تبدیل شوند. ما معتقدیم که روش ارائه شده ما، هم انعطاف‌پذیری و هم امنیت سیستم‌های سایبری سنتی و همچنین سیستم‌های سایبری-فیزیکی هوافضا را افزایش می‌دهد و در نتیجه رویکرد جامع امنیت سایبری ما را متحول می‌کند.

استراتژی طراحی دفاع در عمق ماهواره

«دفاع در عمق» راهبردی است که مدت‌ها قبل از عصر اطلاعات وجود داشته است. در قرون وسطی، قلعه‌هایی ساخته می‌شدند که توسط خندق‌ها و دیوارهای بیرونی احاطه شده بودند و برج‌های دیده‌بانی برای فراهم کردن سطوح مختلف دفاع برای ساکنان داخل

آنها ساخته می‌شدند. اصول اجرای دفاع‌های لایه‌ای و چندگانه نیز به عنوان یک رویکرد برتر برای ایمن نگه داشتن زیرساخت‌های فناوری اطلاعات در برابر تهدیدات سایبری به طور گسترده شناخته شده است. با این حال، امنیت به این شکل اغلب در طراحی سیستم‌های سایبری که هدف تجاری و هزینه در اولویت‌های بالاتری قرار دارند، در اولویت بعدی قرار می‌گیرد. اجرای صحیح یک راهبرد دفاع در عمق به این روش امکان‌پذیر نیست. ایجاد روستایی را تصور کنید که در آن اولویت به حداکثر رساندن دسترسی به زمین‌های کشاورزی و مسکن برای روستاییان داده می‌شود. اگر امنیت روستا قبل از فرآیند ساخت و ساز در نظر گرفته نشود، برج‌های دیده‌بانی نمی‌توانند در مکان‌های بهینه‌ای که خانه‌ها و مزارع زمین را اشغال کرده‌اند، قرار گیرند. خندق‌ها و دیوارهای بیرونی ممکن است به دلیل کمبود منابع مالی کوتاه، باریک یا ناقص شوند یا شاید به دلیل زمین غیرقابل ساخت، کاملاً کنار گذاشته شوند. به طور مشابه، در سیستم‌های فناوری اطلاعات، اجرای دفاع عمیق پس از ایجاد زیرساخت بسیار پرهزینه است. آزمایش‌های نفوذ که بر روی زیرساخت‌های ایجاد شده انجام می‌شوند، می‌توانند آسیب‌پذیری‌های سیستم‌های سایبری را آشکار کنند، اما در نهایت می‌توانند به راه‌حل‌های پراکنده‌ای منجر شوند که سعی در پوشش مسائل بزرگ‌تر ذاتی در طراحی و پیاده‌سازی اولیه آنها دارند. باز هم، با توجه به اینکه طراحی مجدد و اجرای یک راه‌حل کارآمد بسیار پرهزینه است، ملاحظات امنیتی باید در مرحله طراحی چرخه عمر سیستم‌های سایبری در نظر گرفته شوند.

مسلماً، گفتن این پیشنهاد بسیار آسان‌تر از انجام دادن آن است. با افزایش تعداد راه‌حل‌های فناوری اختصاصی و متن‌باز که باید برای ارائه خدمات با هم کار کنند، دستیابی به سازگاری می‌تواند دشوار باشد. در نظر گرفتن یک استراتژی دفاع در عمق برای امنیت می‌تواند پیچیده و پرهزینه شود. بیایید نگاهی به فرآیند طراحی ماهواره‌ای بیندازیم که می‌تواند برخی از این نگرانی‌ها را کاهش دهد.

استراتژی طراحی و چرخه عمر Satcom

چرخه عمر SatComs با یک فرآیند طراحی آغاز می‌شود که قادر به ساده‌سازی ادغام قطعات از فروشندگان متعدد مورد نیاز برای برآورده کردن الزامات پیچیده و حیاتی مأموریت است.

۱.۴ طراحی اولیه

این مرحله آغاز مدل‌سازی سیستم است که با بحث تیم‌ها در مورد امکانات و گزینه‌های موجود برای برآورده کردن الزامات پروژه، تکمیل می‌شود. نکته مهم این است که رابط بین زیرسیستم‌ها مورد بحث و بررسی قرار می‌گیرد. نگرانی‌های امنیتی باید در این مرحله مطرح شوند زیرا سناریوهای احتمالی در نظر گرفته می‌شوند تا دسترسی به خدمات تحت هر شرایطی به حداکثر برسد. کل چرخه عمر سیستم در این مرحله مورد بحث قرار می‌گیرد و درک می‌شود که مأموریت آن می‌تواند یک دهه یا بیشتر طول بکشد.

۲.۴ طراحی بحرانی

در این مرحله، طرح‌های ساخت فضاپیما و سایر زیرسیستم‌ها نهایی و مستندسازی می‌شوند. ۸ قبل از شروع ساخت اجزاء، ملاحظات امنیتی به طور کامل پیاده‌سازی شده و ارزیابی ریسک برای درک کامل پیامدهای خطرات امنیتی انجام شده است. این مرحله با بررسی مشتری به پایان می‌رسد که در آن الزامات پروژه، از جمله امنیت، بررسی می‌شود. اگر نگرانی‌هایی در مورد طراحی وجود

داشته باشد، طرح بررسی، تنظیم و بار دیگر برای بررسی مشتری ارائه می شود. این رویکرد طراحی تکراری صرف نظر از مدل توسعه مورد استفاده برای مدیریت چرخه عمر مخابرات ماهواره ای، وجود دارد.

۳.۴ تست اجزا و رابط کاربری

هنگامی که اجزا ساخته می شوند، به طور مستقل آزمایش می شوند تا از عملکرد صحیح و پیاده سازی طرح تکمیل شده اطمینان حاصل شود. این مرحله دوباره توسط مشتری بررسی می شود تا عملکرد صحیح تأیید شود.

۴.۴ یکپارچه سازی سیستم ها و آزمایش یکپارچه سازی

پس از تأیید عملکرد هر زیرسیستم مطابق با مشخصات مشخص شده، زیرسیستم ها برای تکمیل یک سیستم SatCom عملیاتی به هم متصل می شوند. قبل از تحویل، محصول یکپارچه از نظر عملکرد آزمایش می شود. علاوه بر این، یک آزمایش نفوذ انجام می شود تا تأیید شود که تمام اقدامات امنیتی موجود عملیاتی هستند. برای نهایی کردن فرآیند ساخت، یک بررسی مشتری انجام می شود.

۵.۴ درس های چرخه عمر Satcom در فناوری اطلاعات

با توجه به هزینه بالای پروژه های SatCom و خطرات ناشی از خرابی اجزای فضاپیما، دلایل چنین فرآیند طراحی، آزمایش و تحلیل فشرده ای در طول ساخت سیستم آشکار است. همین اصول، در صورت اعمال در سایر سیستم های فناوری اطلاعات، طول عمر زیرساخت را به حداکثر رسانده و همچنین استحکام دفاعی عمیقی را از همان ابتدا فراهم می کند.

به عنوان یک مثال ساده، می توانیم توسعه یک برنامه وب را در نظر بگیریم. برای راه اندازی این سرویس، چندین مؤلفه یا زیرسیستم وجود دارد که باید در نظر گرفته شوند. یک برنامه وب به یک وب سرور، پایگاه داده، شبکه، سیستم عامل و احتمالاً چارچوب، زبان برنامه نویسی یا سایر بسته های نرم افزاری نیاز دارد. در مرحله طراحی، می توانیم امنیت را در هر یک از این زیرسیستم ها در نظر بگیریم و قبل از ادغام آنها، بهترین شیوه ها را برای دفاع از آنها به صورت جداگانه تعیین کنیم. اگر طراحی ما به گونه ای مهندسی شده باشد که طول عمر کل پروژه را در بر بگیرد، می توانیم نیازهای آینده را پیش بینی کنیم و از ابتدا استحکام مورد نیاز را تعیین کنیم. این امر امنیت را افزایش می دهد زیرا نیازی به انجام ارتقاءهای اساسی زیرساخت در مراحل عملیاتی چرخه عمر برنامه وب نخواهیم داشت. این امر مفید است زیرا چنین ارتقاءهایی ممکن است با الزامات امنیتی اولیه ما مطابقت نداشته باشند یا ممکن است مشکلات امنیتی جدیدی را ایجاد کنند که نیاز به اصلاح در آینده داشته باشند.

۶.۴ بهبود چرخه عمر SatCom

در حالی که ما مزایای پیاده سازی استراتژی های چرخه عمر SatCom را در سایر سیستم های فناوری اطلاعات مشاهده می کنیم، مایلیم استراتژی های SatCom را به گونه ای تقویت کنیم که هم برای صنعت SatCom و هم برای جامعه گسترده تر فناوری اطلاعات مفید باشد.

۷.۴ تست نفوذ

همانطور که قبلاً ذکر شد، پس از ادغام زیرسیستم ها، یک تست نفوذ روی سیستم SatComs انجام می شود. اگرچه این مرحله نباید حذف شود، اما پیشنهاد می کنیم که هر زیرسیستم قبل از ادغام نهایی، یک تست نفوذ انجام دهد. در واقع، با ساخت اجزا، تست های نفوذ باید در پایین ترین سطح ممکن انجام شوند.

این کار، استراتژی دفاع در عمق را که در ابتدا برنامه ریزی شده بود، تأیید می کند. هرچه زیرسیستم ها و اجزای بیشتری در یک سیستم وجود داشته باشد، ارزیابی کامل آن با تست نفوذ دشوارتر است. اگرچه ممکن است در یک تست نفوذ، آسیب پذیری های



زیادی کشف شود، اما هیچ راهی برای تعیین اینکه آیا همه آسیب‌پذیری‌ها شناسایی شده‌اند یا خیر، وجود ندارد. تجزیه تست برای ارزیابی زیرسیستم‌ها هنگام عملیاتی شدن، دقت ارزیابی امنیتی را افزایش می‌دهد. سیستم‌های مخابرات ماهواره‌ای را تضعیف کرده و از پیاده‌سازی سیستم‌های ناامن جلوگیری می‌کند. به طور مشابه، یک پروژه فناوری اطلاعات در مرحله توسعه زیرمولفه، در طراحی تغییراتی که ممکن است در نتیجه توصیه‌های تست نفوذ نیاز به اجرا داشته باشند، بسیار انعطاف‌پذیرتر است.

زیرساخت مخابرات ماهواره‌ای علاوه بر نحوه طراحی و استقرار مخابرات ماهواره‌ای، نحوه راه‌اندازی زیرساخت آنها نیز ذاتاً امن‌تر از سیستم‌های سایبری معمولی است. زیرسیستم‌های مختلفی وجود دارند که برای پشتیبانی از مأموریت مخابرات ماهواره‌ای با یکدیگر همکاری می‌کنند. هر یک از این زیرسیستم‌ها نقش خاصی ایفا می‌کنند و در صورت امکان، جداگانه عمل می‌کنند.

۱.۵ فضاپیما

فضاپیما واحدی است که مسئول پشتیبانی و محافظت از محموله‌ای است که مأموریت مورد نظر را انجام می‌دهد. همچنین تجهیزات ارتباطی دیگری را برای تعامل با سیستم‌های کنترل ماهواره‌ای زمینی و سیستم‌های کنترل محموله در اختیار دارد.

۲.۵ سیستم‌های کنترل ماهواره - SCS

سیستم‌های کنترل ماهواره (SCS) مسئول عملکرد فضاپیما هستند. آنها بر کنترل‌های پیشران، نیرو، محیط زیست و تشخیصی نظارت و مدیریت می‌کنند. این اجزا اغلب به عنوان سیستم‌های تله‌متری، ردیابی و فرماندهی (TT&C) شناخته می‌شوند. TT&C از ایستگاه‌های زمینی که از طریق سیستم‌های باند پایه با فضاپیما ارتباط برقرار می‌کنند، اداره می‌شود.

۳.۵ سیستم‌های کنترل محموله - PCS

سیستم‌های کنترل محموله (PCS) مستقیماً با محموله‌های ماهواره‌ای تعامل دارند. محموله به طور خاص شامل تجهیزاتی است که برای انجام مأموریت برنامه مورد نیاز است. به عنوان مثال، در یک مأموریت پخش تلویزیونی تجاری، محموله شامل فرستنده‌های



لازم برای پخش برنامه‌های تلویزیونی است. PCS بر عملکرد محموله نظارت و مدیریت می‌کند و دسترسی به سرویس را تضمین می‌کند.

۴.۵ سیستم‌های باند پایه - BBS

سیستم‌های باند پایه (BBS) شامل تجهیزات ارتباطی هستند که در توضیحات زیرسیستم‌های قبلی پوشش داده نشده‌اند و می‌توانند شامل آنتن‌های زمینی، سیستم‌های کامپیوتری که از محموله و سایر سخت‌افزارهای ارتباطی استفاده می‌کنند، باشند.

۶.۵ سیستم‌های مدیریت شبکه - NMS

سیستم‌های مدیریت شبکه، امنیت و دسترسی شبکه‌های زمینی به هم پیوسته را که در آنها ایستگاه‌های پایه و سایر تجهیزات درگیر هستند، حفظ می‌کنند.

زیرسیستم‌های شرح داده شده همگی برای تکمیل سیستم مخابرات ماهواره‌ای حیاتی هستند، زیرا هر کدام نقش مهمی در عملکرد آن ایفا می‌کنند. با این حال، با درک اینکه نقش‌های آنها کاملاً متفاوت است، این زیرسیستم‌ها باید ایزوله باقی بمانند، مگر در مواردی که برای برآورده کردن الزامات مأموریت ضروری باشد.

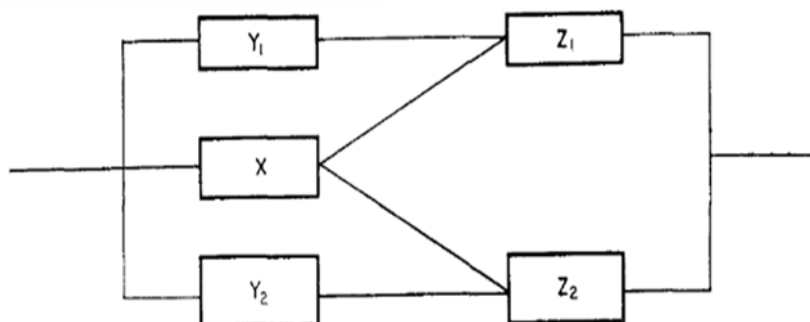
این ایزوله‌سازی بهترین شکل امنیت را در برابر مهاجمان خارجی فراهم می‌کند. اگر دسترسی بین شبکه‌ای بین زیرسیستم‌ها کم یا بدون دسترسی باشد، احتمال موفقیت یک حمله سایبری بسیار کمتر است.

این روش همچنین ذاتاً چندین لایه امنیتی را فراهم می‌کند. اگر یک مهاجم بتواند سیستم مدیریت شبکه را دور بزند و به درستی از سایر زیرسیستم‌ها ایزوله شود، مهاجم همچنان قادر به نفوذ به فضاپیما نخواهد بود زیرا زیرسیستم‌های PCS و SCS به شبکه‌های ایستگاه پایه متصل نخواهند بود. البته این راه حل ایده‌آل است و گاهی اوقات چنین ایزوله‌سازی با توجه به الزامات مأموریت خاص امکان‌پذیر نیست. در جایی که این ایزوله‌سازی امکان‌پذیر نباشد، ورود تک نقطه‌ای بین شبکه‌ها توصیه می‌شود.

۷.۵ سیستم‌های افزونه

درون فضاپیما، اجزای حیاتی مأموریت بسیاری وجود دارد که در محموله و سایر اجزای TT&C که برای عملکرد مناسب لازم هستند، دخیل هستند. از آنجایی که این اقلام را نمی‌توان در اواسط مأموریت تعویض یا تعمیر فیزیکی کرد، اگر قرار است ماهواره در طول چرخه عمر خود به طور کافی عمل کند، باید ملاحظات زیادی در مورد پیاده‌سازی چنین دستگاه‌هایی در نظر گرفته شود. برای این منظور، سیستم‌های افزونه موازی اغلب برای کمک به بازیابی از خرابی اجزا پیاده‌سازی می‌شوند. شکلی که رابطه بین قابلیت اطمینان یک جزء و قابلیت اطمینان کلی سیستم را نشان می‌دهد، نمودار بلوکی نامیده می‌شود. ما فضاپیما را به زیرسیستم‌های داخلی تقسیم می‌کنیم و مسیرهایی ایجاد می‌کنیم که روش‌های ممکن برای دستیابی به مأموریت ماهواره را شرح

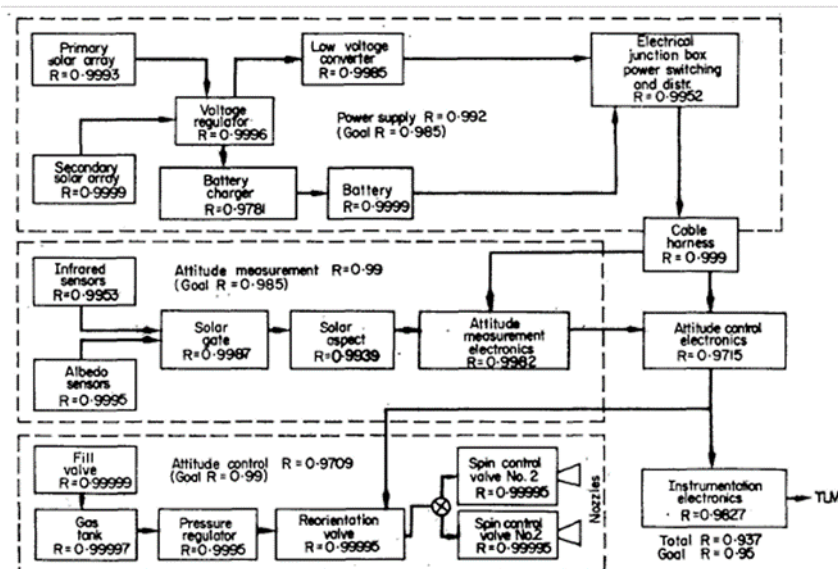
می‌دهند. ماموریت در صورتی موفقیت‌آمیز است که مسیری از یک انتهای نمودار به انتهای دیگر آن کاربردی باشد. یک مثال ساده در زیر نشان داده شده است:



شکل ۱ - یک نمودار بلوکی ساده که افزونگی زیرمولفه را نشان می‌دهد (داونی، ۱۹۷۰)

در مثال بالا، مسیرهای سرویس چندگانه امکان وقوع خرابی چندین قطعه را فراهم می‌کنند، در حالی که همچنان در دسترس بودن سرویس حفظ می‌شود. در صورت خرابی قطعه X و قطعه Z_2 ، قطعات Z_1 و Y_1 برای تکمیل ماموریت ماهواره در دسترس خواهند بود. روش شرح داده شده یک رویکرد افزونگی ساده ۱:۱ نیست. همچنین این استراتژی افزونگی نیاز به خرابی حداقل دو (به احتمال زیاد سه) قطعه قبل از از دسترس خارج شدن سرویس دارد. باز هم، دستیابی به این سناریوی ایده‌آل همیشه امکان‌پذیر نیست، اما تلاش برای پیکربندی بهینه قطعات، شانس موفقیت ما را افزایش می‌دهد. در ارزیابی معماری ماهواره، در دسترس بودن هر زیرسیستم فضاپیما با دقت در نظر گرفته می‌شود و احتمال قابلیت اطمینان قطعه (R) اندازه‌گیری می‌شود. این امر امکان استفاده از یک مدل ریاضی را

فراهم می کند که احتمال تکمیل موفقیت آمیز ماموریت را پیش بینی می کند. نمودار زیر یک نمودار بلوکی امکان سنجی ماهواره های معمولی است.



شکل ۲ - نمودار بلوکی معمول امکان سنجی ماهواره (داونی، ۱۹۷۰)

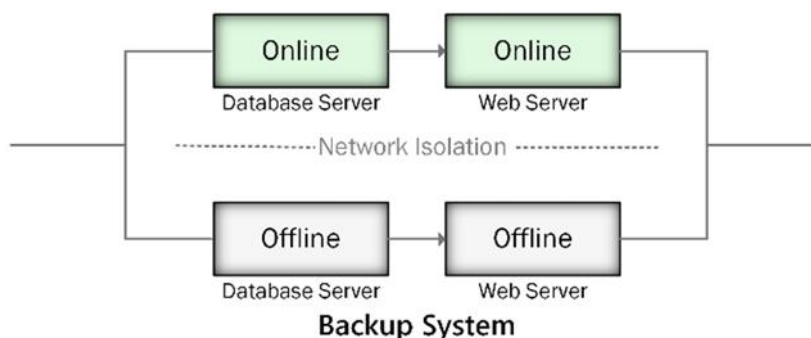
۸.۵ درس های زیر ساخت Satcom در فناوری اطلاعات

در یک محیط فناوری اطلاعات معمولی، اجزای زیادی وجود دارند که با هم کار می کنند تا یک "راهکار عملی" ایجاد کنند. علاوه بر این، روش های زیادی نیز برای اتصال این اجزا وجود دارد. در جهانی که اتصال گسترده تر اغلب ساده ترین روش پیاده سازی در پروژه های فناوری اطلاعات است، ما دسترسی بسیار بازاری بین سیستم ها و خدمات نسبت به آنچه لازم است، پیدا می کنیم. این اعتماد بین این سرویس ها و شبکه هایی که به آنها متصل هستند، "بردارهای حمله چندگانه" را برای هکرها ایجاد می کند تا از آنها سوءاستفاده کنند. اگر به دنبال جداسازی زیرسیستم ها باشیم و "یک نقطه ورود واحد" بین این زیرسیستم ها ایجاد کنیم، می توانیم یک زیرساخت دفاعی عمیق ایجاد کنیم که در برابر حمله بسیار مقاوم تر است.

در حالی که اتخاذ یک رویکرد ریاضی دقیق برای ارزیابی ریسک خرابی زیرسیستم های فناوری اطلاعات ممکن است رویکرد ایده آلی نباشد، درک روش های افزودنی مورد استفاده در ماهواره ها می تواند به ما در حفظ دسترسی به خدمات حتی در بحبوحه یک حمله سایبری کمک کند.

بیا باید مورد ساده یک وب سرور با یک سرور پایگاه داده مرتبط را بررسی کنیم. متأسفانه، سرویس های زیادی وجود دارند که در آنها پایگاه داده و وب سرورها روی یک دستگاه (فیزیکی یا مجازی) نصب شده اند. این یک نقطه شکست واحد برای سرویس ما ایجاد می کند و در صورت حمله سایبری به دستگاه، نیاز به رویکرد «قرنطینه، حل و

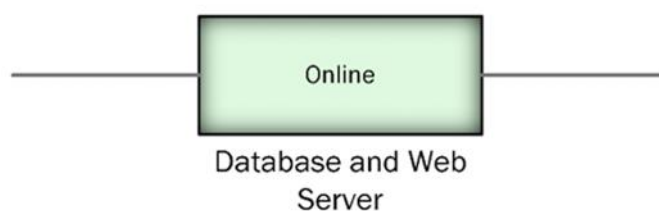
فصل، اصلاح» برای بازیابی سیستم دارد. برای رفع نقص پایگاه داده یا وب سرور، سرویس باید آفلاین شود. در این حالت، نمودار بلوکی به شکل زیر خواهد بود:



شکل ۲ - نمودار بلوکی نقطه شکست تکی

در یک سناریوی خوب برنامه ریزی شده، زیرساخت فناوری اطلاعات شامل سرورهای منحصر به فرد برای زیرسیستم‌ها و یک سیستم پشتیبان است که قرار است در صورت از دسترس خارج شدن یا به خطر افتادن سیستم‌های اصلی، راه اندازی شود. سیستم‌های اصلی و پشتیبان از یکدیگر جدا شده‌اند که به یک استراتژی دفاعی عمیق کمک می‌کند. این یک راه حل بسیار بهتر است، اما مستلزم آن است که در صورت به خطر افتادن یا غیرفعال شدن یک زیرسیستم، کل سیستم اصلی از کار بیفتد. همچنین مقرون به صرفه نیست زیرا سیستم پشتیبان تا زمانی که سیستم اصلی از کار نیفتد، هیچ هدف مفیدی ندارد:

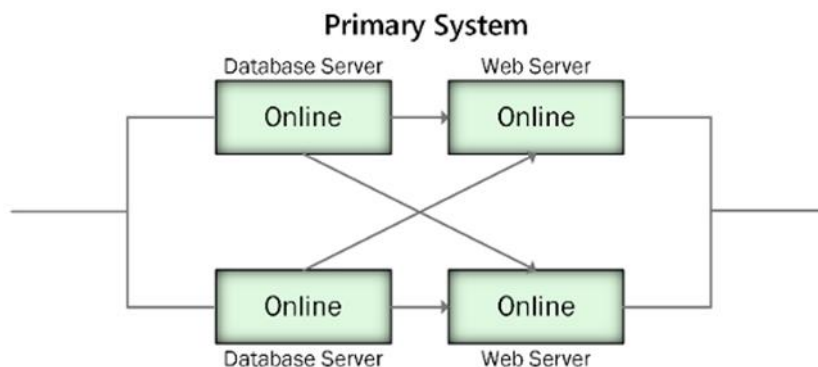
Primary System



شکل ۳ - نمودار بلوکی سیستم افزونه

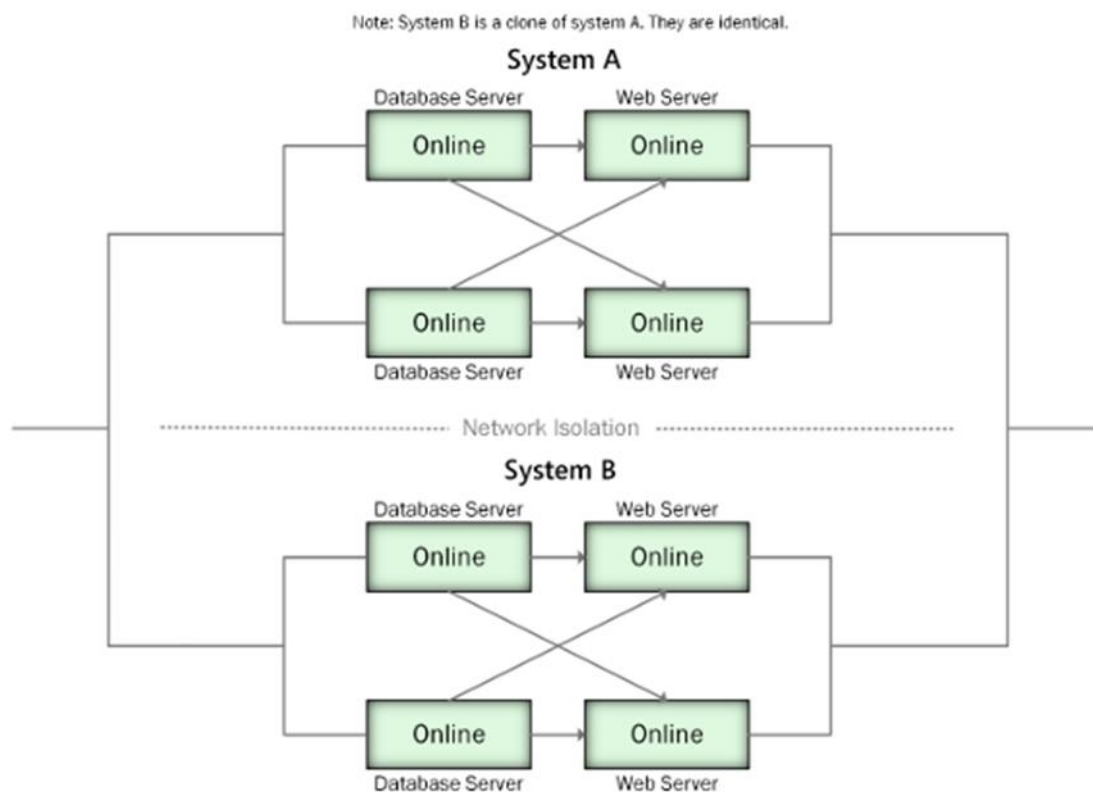
برای به حداکثر رساندن دسترسی به خدمات و کاهش هزینه‌ها، می‌توانیم اصل مسیرهای چندگانه را از مخابرات ماهواره‌ای گرفته و آن را به شیوه‌ای معنادار در زیرساخت برنامه‌های وب خود اعمال کنیم. ما این کار را با فعال کردن

تمام منابع موجود برای پشتیبانی از خدمات مورد نظر و اجازه دادن به هر سیستم مستقل برای به اشتراک گذاشتن منابع زیرسیستم در صورت خرابی یک جزء انجام می دهیم:



شکل ۴ - نمودار بلوکی که مسیرهای چندگانه را نشان می دهد

سپس، با استفاده از چندین شبکه ایزوله برای افزودن به استراتژی دفاع در عمق خود، می توانیم از طریق بخش بندی، از زیرساخت های خود بیشتر محافظت کنیم. می توانیم این کار را بسته به میزان منابع مورد نیاز برای ارائه خدمات با عملکرد بهینه، به تعداد دفعات دلخواه انجام دهیم:



شکل ۵ - نمودار بلوکی مسیرهای چندگانه ایزوله

در این سناریوی ساده، ما استراتژی‌های مورد استفاده در صنعت مخابرات ماهواره‌ای را برای ایجاد یک محیط فناوری اطلاعات امن، قوی و با حداکثر دسترسی‌پذیری، اعمال و ترکیب کرده‌ایم. ما این را روش‌شناسی «مسیرهای چندگانه ایزوله» برای سیستم‌های فناوری اطلاعات می‌نامیم. مثالی که بررسی کرده‌ایم بسیار ساده است زیرا معمولاً زیرمولفه‌ها و دستگاه‌های شبکه و زیرساخت‌های بسیار بیشتری وجود دارند که در اینجا در نظر گرفته نشده‌اند. با این حال، ما معتقدیم که این دیدگاه انتزاعی می‌تواند ارزش کاربردی معناداری در طراحی انواع سیستم‌های فناوری اطلاعات آینده که خدمات مختلفی ارائه می‌دهند، داشته باشد. لازم به ذکر است که هر شبکه ایزوله از نظر عملکرد و خدمات یکسان است، با این حال، تفاوت‌های یکپارچه‌سازی امنیتی بین هر یک وجود دارد تا احتمال به خطر افتادن چندین شبکه را کاهش دهد. به عنوان مثال، نام‌های کاربری و رمزهای عبور مورد استفاده در سیستم A ممکن است با نام‌های کاربری و رمزهای عبور سیستم B متفاوت باشد یا شبکه‌ها ممکن است در مکان‌های جغرافیایی متفاوتی مستقر شده باشند.

۹.۵ مزایای یک زیرساخت چند مسیره ایزوله

- ✓ مزایای اتخاذ این رویکرد در زیرساخت فناوری اطلاعات به شرح زیر است:
- ✓ شبکه‌های ایزوله در برابر به خطر افتادن کامل زیرساخت مقاوم می‌شوند که به سرویس‌ها اجازه می‌دهد در صورت وقوع یک حمله سایبری فاجعه‌بار، فعال باقی بمانند.
- ✓ مسیرهای سرویس چندگانه به زیرسیستم‌ها اجازه می‌دهند بدون اختلال در عملکرد سیستم، از کار بیفتند. زیرسیستم‌ها را می‌توان در حین ارائه تداوم سرویس، جایگزین کرد.
- ✓ مقرون به صرفه بودن مسیرهای چندگانه ایزوله بالا است زیرا همه اجزای زیرساخت در همه زمان‌ها فعال هستند و می‌توانند در مأموریت مورد نظر مشارکت کنند.
- ✓ بخش‌بندی شبکه‌ها به محافظت در برابر حملات انکار سرویس توزیع شده (DDOS) کمک می‌کند.

۶. پیامدهای آموزش فناوری اطلاعات

در این مقاله، ما در مورد روش‌هایی که درس‌های آموخته‌شده از صنایع هوافضا و فناوری اطلاعات می‌توانند در سناریوهای جدید یا موجود به طور متقابل سودمند باشند، بحث کرده‌ایم. متأسفانه، در آموزش دانشجویان و متخصصان در زمینه‌ی آوردن امنیت سایبری به خط مقدم حوزه‌های خود و به‌کارگیری آن به روش‌های مؤثر، شکاف‌هایی وجود دارد. این امر با عدم توجه به دفاع در برابر حملات سایبری در شبکه‌های ماهواره‌ای جدید که در آن‌ها TCP/IP و سایر پروتکل‌های آشنا برای متخصصان فناوری اطلاعات وجود دارد و همچنین عدم ارتباط بین مهندسان در رابطه با ساخت سیستم‌های سایبری در حوزه‌های هوافضا و فناوری اطلاعات، مشهود است. همانطور که از ایده‌های ارائه شده در این مقاله مشهود است، با گرد هم آوردن افراد در زمینه‌های نزدیک به هم برای نوآوری در روش‌های دفاعی که از زیرساخت‌های حیاتی و سایر زیرساخت‌های ما محافظت می‌کنند، می‌توان پیشرفت زیادی حاصل کرد. اگر این کار را نکنیم، با به هم پیوسته‌تر شدن جهان، خود را در معرض خطر قرار می‌دهیم. صنایعی که زمانی نگرانی کمی در مورد حملات سایبری داشتند، اکنون باید بسیار بیشتر از تهدیدات آگاه شوند و استراتژی‌های دفاعی را تدوین کنند که به بهترین نحو از دارایی‌های آنها محافظت کند. در مهندسی و فناوری، امنیت سایبری تنها بخش کوچکی از سطح آموزشی را که در برنامه درسی امروز در نظر گرفته شده است، اشغال می‌کند. لازم است که



فناوری‌های جدید با در نظر گرفتن امنیت توسعه یابند. امنیت نه تنها باید در خط مقدم توسعه زیرساخت‌ها، بلکه در آغاز نوآوری و اختراع نیز در نظر گرفته شود. این بدان معناست که دانشجویان ما باید پیشینه لازم برای آگاهی از امنیت و درک خطرات احتمالی مرتبط با فناوری‌های جدید را داشته باشند.

بحث و نتیجه‌گیری

ما در مورد روش‌هایی که صنعت مخابرات ماهواره‌ای به قابلیت اطمینان و امنیت ماهواره نزدیک شده است و چگونگی اعمال آنها در سایر سیستم‌های فناوری اطلاعات بحث کرده‌ایم. فرآیندهای طراحی و چرخه عمر سیستم ماهواره‌ای می‌تواند متخصصان فناوری اطلاعات را تشویق کند تا با انجام بررسی‌های متعدد، آزمایش نفوذ زیربخش‌ها و برنامه‌ریزی دقیق کل چرخه عمر زیرساخت در صورت امکان، امنیت را در کنار در دسترس بودن، در اولویت قرار دهند. علاوه بر این، ما کشف کردیم که رویکرد معماران ماهواره به قابلیت اطمینان فضاپیما می‌تواند امنیت سیستم‌های فناوری اطلاعات ما را بهبود بخشد، اگر بتوانیم از مسیرهای سرویس چندگانه در مکانیسم‌های تولید خود استفاده کنیم. ما همچنین بر لزوم ارائه امنیت در اوایل آموزش دانشجویان خود تأکید کرده‌ایم تا ذهنیت امنیتی را در مهندسان و تکنسین‌های جدید تشویق کنیم.

کاربرد مسیرهای چندگانه ایزوله در فرآیند طراحی همراه با آزمایش‌های نفوذ زیرسیستم و سیستم کامل، بسته به پروژه متفاوت خواهد بود و نیاز به اعتبارسنجی در سناریوهای دنیای واقعی دارد. این امر فرصت کافی برای انجام کارهای اضافی در این زمینه را فراهم می‌کند.

منابع

- 1)Jii WJL. Defending a New Domain The Pentagons Cyberstrategy. Council on Foreign Relations. 2010;89(5):97-108.
- 2)National Cyber Security Strategies in the World. European Union Agency for Network and Information Security.
- 3)Register F. Executive Order 13636—Improving Critical Infrastructure Cybersecurity. National Archives and Records Administration. 2013;78(33):1–8.
- 4)Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014. 2014:1–41.
- 5)Update on Sony Investigation. FBI National Press Office. 2014.
- 6)Fulghum DA. Cyber-Scrimmage. Aviation Week & Space Technology. 5/17/2010, Vol. 172 Issue 19. 2010 May:26–27.
- 7)Jones B. Global Information Assurance Certification Paper. GIAC. 2005.
- 8)Rowe D, Rowe K. Space - The Final Cyber-Frontier 2012.
- 9)Downey MJ. Satellite reliability. Microelectronics and Reliability. 1970;9:271–282.