5. چالش های فرهنگی

خلاصه

این فصل توضیح دهنده ی یک شکاف فرهنگی بین پرسنل نیروگاه هسته ای یا مهندسان OT و پرسنل امنیت سایبری یا مهندسان IT است. شیوه های متفاوت فکری آنها باعث اولویت های مختلفی می شود که باهم منطبق نیستند و می توانند باعث اصطکاک شوند. یکی از این پیامدها این است که پرسنل نیروگاه هسته ای معمولا رویه های امنیت سایبری را درک نمی کنند. به علاوه رویه ها همیشه به روشنی نوشته نمی شوند و نتیجتا پرسنل نیروگاه هسته ای نمی دانند در هنگام یک رویداد امنیتی سایبری چه کسی را خبر کنند و بنابراین توصیه ها و نیازمندی ها را به صورتی که توسط مهندسان IT خواسته شده تفسیر نمی کنند. این مشکلات ارتباطی به دلیل تعاملات محدود بدتر هم می شوند زیرا کسانی که مسئول امنیت سایبری هستند در محل حضور ندارند. علاوه بر این آموزش های امنیت سایبری در تاسیسات اتمی معمولا کافی نیست و عدم وجود مانورهای آزمایشی بدین معناست که پرسنل نیروگاه هسته ای هیچ فرصتی را برای تمرین این رویه ها ندارند.

نگرانی دیگری که در این مصاحبه ها گفته شده است این است که امنیت در تاسیسات اتمی بیشتر واکنشی است تا فعال. در حالی که این وضعیت ممکن است در سایر مکان ها جوابگو باشد در ارتباط با امنیت سایبری پرسنل در تاسیسات هسته ای ممکن است تا هنگام وقوع یک حمله ی سایبری از وجود آن مطلع نشوند. ترکیب این عوامل که در بالا گفته شد این را می رساند که نیروگاه های هسته ای ممکن است برای یک وضعیت اورژانسی مرتبط با امنیت سایبری به خصوص اگر در خارج از زمان های کاری عادی روی دهد به اندازه کافی آمادگی نداشته باشند.

اولویت های متناقض و شکاف های فرهنگی

پرسنل نیروگاه هسته ای که معمولا مهندسان OTهستند و پرسنل امنیت سایبری که مهندسان ITدر نظر گرفته می شوند، معمولا اولویت های متناقضی دارند. قوانین انضباطی OT معمولا در ارتباط با عملیات کاری یک نیروگاه است –مانند سیستم های کنترل صنعتی، شامل مدیریت از راه دور پمپ ها و شیرها- در حالی که ITمعمولا در ارتباط با کامپیوترها و شبکه هاست. هرگروه اولویت ها و روش فکری متفاوتی دارد. در موارد زیادی این چارچوب های اهمیت با همدیگر برخورد می کنند و باعث بین درگیری دو گروه می شوند. آنها معمولا ممکن است حتی متوجه نشوند که روشهایشان متفاوت است و این به صورت اجتناب ناپذیری باعث برخورد می شود.

ایمنی در برابر امنیت سایبری. از نظر تاریخی اولویت اصلی مهندسان OT اطمینان از عملکرد ایمن و بهینه ی نیروگاه بوده است اما برای پرسنل امنیت سایبری (یا مهندسان IT) امنیت در اولویت است.

منبع 5 توضیح دهنده ی یک جلسه اخیر آژآنس انرژی اتمی است که در آن مهندسان OT (همان مهندسان ایمنی) و مهندسان IT (همان مهنسان ایمنی) در مورد آن چشم اندازهای متفاوت که باعث می شود تنوانند همدیگر را درک کنند بحث کرده است:

مهندسان ایمنی از مهندسان امنیت درخواست اضافه کردن امنیت به یک سیستم را دارند اما همچنین به آنها می گویند که شما نمی توانید به بقیه ی تست ها دست بزنید، ما 19 تست انجام داده ایم و شما تست آخر هستید، تست 20. آنها می خواستند که اطمینان یابند که مهندسان امنیت هیچ کدام از تست های ایمنی قبلی را باطل نمی کنند. در کل آن ها می گویند که فقط مطمین شوید که برای ما درست است و هیچ کدام از تست های پیشین را نقض نکنید.

در حقیقت در این سناریو به سادگی امکان برخورد با امنیت به عنوان یک بخش اضافی بر ایمنی وجود ندارد زیرا مهندسان IT نمی‌توانند امنیت را بدون احتمال ایجاد یک تغییر که ایمنی را نقض می‌کند وارد کنند. برای نمونه یک کنترل کننده شیر ممکن است یک وضعیت ایمنی با جزییاتی داشته باشد که توسط نیروگاه تأیید شده است اما با ایمنی کم و یا بدون ایمنی در برابر تداخلات است. اگر نیروگاه تصمیم بگیرد که امنیت را به این کنترل کننده شیر بیافزاید، انجام این کار می‌تواند باعث نقض بعضی از تست های ایمنی شود که تا کنون انجام شده است و یا ممکن عدم انطباقهای غیر منتظره ای مابین سیستم‌های ایمنی و سیستمهای امنیت وجود داشته باشد. سیستم در آن صورت ممکن است به صورتی رفتار کند که دیگر ایمن نباشد. این مخصوصاً در حالتی می‌تواند درست باشد که نیروگاه هسته ای بخواهد کنترل کننده شیر را به شبکه متصل کند تا دسترسی آسانتری به داده‌های تولید شده توسط وسیله داشته باشد.

دلیل این که مهندسان ایمنی درک نمی‌کنند این است که این نه عملی است و نه ممکن، شما نمی‌توانید یک بدون تغییر حالت یک سیستم از آن دفاع کنید. و بنابراین هنگامی که مهندسان ایمنی می‌گویند ٬شما نمی‌توانید وضعیت را تغییر دهید٬ مهندسان ایمنی می‌گویند ٬در این صورت ما نمی‌توانید از آن دفاع کنیم٬ (منبع ۵)

دسترسی در برابر امنیت. مهندسان OT تأمین دسترسی (به بیان دیگر کارکردن مداوم نیروگاه) را در اولویت قرار می‌دهند در حالی که پرسنل امنیت سایبری (یا مهندسان IT) همان‌طور که در بالا گفته شد ایمنی را به عنوان نقطه تمرکزشان قرار می دهند.

با وجود این نمی‌توان دسترسی و ایمنی را باهم افزایش داد. برای نمونه وصله کردن (patching) یک سیستم در برابر نقاط ضعف شناخته شده ممکن است به معنی این باشد که سیستم ممکن است در هنگام نصب و آزمایش در دسترسی نباشد (بخش ۶ را ببینید). علاوه بر کاهش دسترسی سیستم، مهندسان OT معمولاً ترجیح می‌دهند که وصله نکنند. از دید یک مهندسی IT، وصله کردن راهی برای افزایش امنیت در برابر تعداد فزاینده ی تهدیدات امنیت سایبری است. در یک مقیاس وسیعتر مهندسان IT می‌توانند در موقعیتی باشند که برای تأمین امنیت یک سیستم تأسیسات نیاز به خاموش کردن نیروگاه برای حذف یک تهدید امنیت سایبری داشته باشند – که به صورت مستقیم با نیازهای مهندسان OT متناقض است.

در طرف دیگر تأسیسات هسته ای در دسترس بودن را به عنوان یک اولویت کلیدی می خواهد. بخش سایبری امنیت را به عنوان یک اولویت کلیدی می‌خواهد و معمولاً آن‌ها به خوبی نمی‌توانند باهم همزیستی داشته باشند. این درگیری واقعی است (منبع ۲۵).

غیرعمدی (تصادفی) در برابر عمدی (مخرب). مهندسان OT معمولاً در فکر جلوگیری از حوادث و سایر اعمال ناخواسته هستند. این نگرانی به صورت مستقیم از تمرکز آن‌ها بر ایمنی نشأت می گیرد. اما برخلاف آن‌ها پرسنل امنیت سایبری (یا مهندسان IT) متمایل به تمرکز بر جلوگیری از اعمال عمدی که امکان آسیب رسانی به نیروگاه را دارند هستند که شامل حملات مخرب است (علاوه بر این آن‌ها به فکر حوادث ناخواسته هم هستند).

تمرکز طولانی مهندسان OT‌ بر ایمنی و محافظت در برابر حوادث به این معنی است که آنان روشهای دقیق تحلیل آماری را توسعه داده اند. آن‌ها با مشکلات با انجام یک تحلیل خطای عادی برخورد می‌کنند که به آن‌ها اجازه می‌دهد که به همه چیز که از نظری تئوری می‌توانند دچار مشکل شوند و احتمالاتی که تمام حوادث ممکن، امکان وقوع دارند و اینکه دلایل پشت آن‌ها چه می‌تواند باشد نگاه کنند. این روش به صورتی در فرهنگ آن‌ها مرکزیت یافته است که آن‌ها از مهندسان IT انتظار دارند که همان نوع تحلیل عادی را به آن‌ها ارایه دهند. اما مهندسان IT برای برخورد با مشکلات به این شیوه پرورش پیدا نکرده اند. آن‌ها نیازمند در نظر گرفتن مسیرهای تهدیدات عمدی هستند که تعداد زیادی دارند و غیر قابل پیش‌بینی هستند و توسط آن تحلیل قابل بررسی نیستند. برای مثال حمله کنندگان ممکن است از آسیپ پذیری های روز صفر و سایر تکنولوژی های حملاتی که تاکنون دیده نشده استفاده کنند و عوامل تهدید جدید می‌تواند ظهور کند.

اصطکاک بین پرسنل نیروگاه هسته ای و پرسنل امنیت سایبری

با داشتن تناقضات اهداف و شیوه فکری پرسنل نیروگاه هسته ای و امنیت سایبری، عجیب نیست که در زمان هایی درجاتی از درگیری خود را مابین آن‌ها نشان می دهد. مصاحبه‌ها با پرسنل از هردو گروه داستان‌هایی را بازگو می‌کند که بیشتر این اصطکاکات را نمایش می‌دهد و بعضی از دلایل پشت آن‌ها را توضیح می دهد.

منبع ۸ تأکید می‌کند که ناخشنودی منهدسان OT از مهندسان IT یک بخش اصلی از چالش امنیت سایبری است:

مشکل همان‌گونه که تکنیکی است به همان اندازه هم فرهنگی و جامعه شناسانه است. یکی از بزرگترین مشگلاتی که داریم این است که – به همان صورت صنعت – پرسنل عملیاتی از IT بیزارند.

منبع 25، یک منهدس IT تلاش می‌کند تا وضعیت را از دید مهندس OT ببیند :

من می‌توانم درک کنم که چرا مدیران نیروگاه هسته ای از ما خوششان نمی‌آید، زیرا آن‌ها فکر می‌کنند که ما درد آور هستیم. ما در آخر یک فرایندی که کار می‌کند می‌آییم (و می‌گوییم که تمام این تمهیدات امنیت سایبری باید اضافه شوند). ما امنیت سایبری را برای محافظت از آن‌ها اضافه می‌کنیم اما از دید آن‌ها منافع این کار دیده نمی شود.

بخشی از مشکل می‌تواند به باوری که در بین بعضی پرسنل نیروگاه هسته ای وجود دارد ارتباط یابد آن‌ها می‌اندیشند امنیت سایبری یک تهدید واقعی را ایجاد نمی‌کند؛ بنابراین تمایل دارند که تمهیدات امنیت سایبری را که توسط مهندسان IT بر آن‌ها تحمیل شده است را به عنوان یک مزاحمت ببینند تا اینکه یک کمک مهم به ایمنی نیروگاه.

منبع ۶،‌یک مهندس OT که برای ۱۰ سال در دو نیروگاه مختلف هسته ای در ایالات متحده کار کرده بود، بخشی از ناراحتی‌ها را در مورد مهندسان IT بازگو می کند. او به صلاحیت آن‌ها باور نداشت، به‌خصوص به این دلیل که آن‌ها به ندرت مهندسی هسته ای هستند و اعتقاد داشت که آن‌ها درک نمی‌کنند که چگونه یک نیروگاه هسته ای کار می کند. او می گوید:

من هیچ وقت قانع نشده‌ام که هنگامی که ما رویه (اضطراری سایبری) را پیاده‌سازی می‌کردیم فرد انجام دهنده آن اصلاً واجد صلاحیت بود. قطعاً به اندازه من صلاحیت نداشت زیرا من آموزش دیده هستم. او ممکن است بزرگترین جادوگر کامپیوتر در جهان باشد اما هیچ ایده ای از اینگه چگونه یک نیروگاه هسته ای کار می‌کند ندارد.

بدون این درک اساسی، از دید او،‌ مهندسان IT نمی‌توانند درک کنند که چرا پایدارسازی راکتور آنقدر ضروری است. نتیجتاً بسیاری از مهندسان IT ممکن است ناراحت شوند اگر پرسنل نیروگاه هسته ای مانع کار آن‌ها بر مسایل IT شوند زیرا آن‌ها باید در ابتدا راکتور را پایدار کنند؛ مهندسان IT درک نمی‌کنند که چرا آن باید در اولویت باشد.

بازه ی بی اعتمادی در حدی است که منبع ۶ تردیداتی را در مورد اینکه آیا او می‌تواند در هنگام وقوع شرایط اورژانسی بر مهندسی IT اعتماد کند اعلام می کند. او می‌گوید که مهندسان IT ، اخلاق حرفه‌ای کافی ندارند و هنچنین می‌گوید: آن‌ها می‌خواهند کار را به سرعت هرچه تمام تر پایان دهند تا بتوانند به خانه بروند. آن‌ها کارکنان تمام وقت (24/7)همانند ما نیستند – منظور او این است که احتمال اینکه مهندسان IT در خارج از ساعات اداری در صورت وقوع پیشامدی در دسترس باشند کمتر است. برخلاف پرسنل نیروگاه هسته ای که به فراخوانی های اورژانسی در نیمه شب عادت دارند، پرسنل امنیت سایبری در برابر مدیران میانی پاسخگو هستند که معمولاً نیاز به برخورد با فراخوانی های خارج از وقت کاری ندارند و این حس می‌شود که آن‌ها به اندازه کافی به طبیعت حساس کارشان آگاه نیستند.

همان منبع دیده است که مهندسان IT معمولاً می‌خواهند کل جزییات مسأله را پیش از تصمیم گیری بدانند و یا در بعضی موارد نیاز به اجازه از مسئول مربوطه در ساختار مدیریتیشان پیش از انجام یک کار دارند – که بدین معناست که در هنگام یک رویداد نمی‌توانند به سرعت تصمیم گیری کنند. علاوه بر این بر خلاف پرسنل نیروگاه هسته ای، پرسنل امنیت سایبری نیازمندی های آمادگی برای وظیفه را ندارند (شامل محدودیت‌های ساعت کاری و قوانین مربوط به مصرف الکل پیش از گزارش برای یک شیفت)،‌بنابراین یک مهندس OT ممکن است نداند که یک مهندس IT پاسخگو برای یک رویداد سایبری در تمام شب بیدار بوده است و یا مریض است.

منبع ۶ بازگو می‌کند که چگونه در نیروگاه هسته ای که او در آن کار کرده است، مهندسان IT مستندات مربوط به رویه های امنیت سایبری را برای پرسنل نیروگاه هسته ای توسعه می‌دادند تا در هنگام یک رویداد سایبری آنچه را که انجام می‌داده آند متوقف کنند و به چیزی دست نزنند و پرسنل امنیت سایبری را فرابخوانند. آن‌ها برای پرسنل نیروگاه هسته ای طبیعت خطرات امنیت سایبری، چگونگی برخورد با آن‌ها یا منطق پشت رویه را توضیح نمی دادند:

ایمنی راکتور همیشه یکی از مسئولیت های مهم من بود. برای تمام رویه های دیگر برای نمونه اگر مشکلی برای پمپ تغذیه روی می داد، فرد مسئول به صورت کامل تمام مراحل و چرایی انجام آن‌ها را درک کرده بود. دلیل این است که در هنگامی که شما به آن مرحله رسیدید و مشکلی در تجهیزات وجود داشت بتوانید یک راه حل پیدا کنید. بنابراین چیزهایی مانند ٬آنچه را که انجام می‌دهید متوقف کنید، به هیچ سیستم کنترل حیاتی دست نزنید، ٬ تعجب برانگیز است.

علاوه بر حالت گفتن آنکه بعضی از پرسنل نیروگاه هسته آن را توهین آمیز می دانند، مشکل دیگری که در این روش وجود دارد این است که بعضی اوقات مشخص است که رویدادی اتفاق افتاده است اما منبع -چه به دلیل یک رویداد امنیت سایبری و چه چیز دیگر – ممکن است نامشخص باشد. بنابراین پرسنل نیروگاه هسته ای نمی‌دانند که آیا باید پرسنل امنیت سایبری را فراخوانی کنند یا نه و اطلاعات محدودی که در مورد برخورد با رویداد های امنیت سایبری دریافت کرده‌اند تشخیص عامل را برایشان مشکل‌تر می کند.

رویه های مبهم

مصاحبه همچنین فاش می‌کند که پرسنل نیروگاه هسته ای معمولاً رویه های امنیت سایبری شامل آن‌هایی که باید در یک وضعیت اضطراری سایبری دنبال کنند را درک نمی کنند. حتی باتجربه ترین پرسنل نیروگاه هسته ای دشواری هایی را در درک رویه های به صورتی که در اسناد نوشته شده است گزارش داده اند.

رویه ها به صورت وحشتناکی گیج‌کننده هستند...من واقعاً رویه را درک نمی کنم. چیزی که من می‌دانم این است که اگر یک رویداد سایبری اتفاق افتاد، اولین قدم این است که باید به اپراتورها بگویم آنچه را انجام می‌دهند متوقف کنند و به هیچ کدام از سیستم‌های کنترل حیاتی دست نزنند. و سپس قدم دوم این است که بعد از اطلاع رسانی به بخش امنیت باید به هرکس از افراد سایبری که آن کال است خبر بدهم. (منبع ۶)

معمولاً به این دلیل است که رویه ها به روشنی نوشته نشده اند. پرسنل نیروگاه هسته ای گزارش می‌دهند که رویه های امنیت سایبری را آن‌چنان دشوار یافته‌اند که نمی‌دانند در هنگام یک رویداد امنیت سایبری به چه کسی اطلاع دهند. در یک مورد جایی که در مستندات رویه ای یک فلوچارت از اینکه در هنگام آن رویدادها از بین افراد امنیت سایبری چه کسی را باید خبر کرد وجود داشت چارت مبهم بود. منبع ۶ اضافه می کند:

مانند این است که، ٬مسئول مهندسان را فراخوانی کن، کسی که فرد دیگری را فراخوانی می‌کند و آن فرد هم فرد دیگری را فراخوانی می کند٬. من هیچ ایده ای از اینکه آن‌ها چه کسانی هستند نداشتم و هیچ وقت مطمین نبودم که فرد صحیح کدام است و کدام متخصص سایبری باید فراخوانده شود.

در حقیقت، دشواری درک رویه محدود به مهندسان OT نیست. مسئولین حراست فیزیکی در نیروگاه هسته ای که باید گاهی نیازمندی های IT را پیاده‌سازی کنند همچنین در درک رویه های امنیت سایبری مشکل داشتند. منبع ۷ می گوید:

چیزی که برای متخصصان ایمنی (هسته ای) خسته‌کننده است این است که بعضی از توصیه‌ها بد نوشته شده اند، مبهم هستند و بی‌معنایند. گاهی اوقات سخت است که فهمید توصیه‌ها چه هستند.

با وجود آنکه مستندات رویه ها توسط مهندسان IT نوشته شده است, با روش و طرز فکر متفاوتشان این بسیار عجیب است. دشواری های پرسنل نیروگاه هسته ای در درک مستندات یک علامت واضح از شکاف فرهنگی است. همان طور که منبع 8 توضیح داده است: یک دلیل اینکه دستورالعمل ها مبهم هستند این است که آنها از دید امنیت IT نوشته شده اند.  
نتایج این مورد این است که تفسیر توصیه ها یا نیازمندی ها توسط پرسنل نیروگاه هسته ای ممکن است بسیار با نیات مهندسان IT متفاوت باشد.  مهندسان OT و IT معمولا معناهای متفاوتی از یک عبارت یکسان می گیرند. برای مثال برای یک مهندس OT یک "عدم سرویس" ممکن است به این معنی باشد که یک پمپ سردکننده اصلی 10000 اسب بخاری در یک نیروگاه هسته ای خاموش شده است. برای یک مهندس IT یک عدم سرویس به این معناست که یک جریان سیل آسای مخرب از داده یک منبع محاسباتی را از دسترس خارج کرده است.به عنوان یک مثال دیگر هرچند رویه های امنیت سایبری به پرسنل نیروگاه هسته ای می گوید که در هنگام یک واقعه به هیچ سیستم کنترل حیاتی دست نزنند, اما مشخص نمی کند که کدام سیستم یا سیستمها باید به عنوان حیاتی در نظر گرفته شود. بنابراین انتظار می رود که پرسنل نیروگاه هسته ای از تشخیص خودشان استفاده کنند و نتیجه گیری های آنها ممکن است با مولفان رویه های امنیت سایبری بسیار متفاوت باشد.  
به صورت مشابه پرسنل امنیت فیزیکی در نیروگاه هسته ای ممکن است سیستم تشخیص نفوذ را به عنوان یک کنترل کننده دروازه یا یک کارت خوان تفسیر کنند. برای یک مهندس IT, یک سیستم تشخیص نفوذ, شبکه را برای ترافیک مشکوک بررسی می کند.  
متخصصان امنیت و IT یک تفسیر متفاوت از اینکه برآورده کردن امنیت IT دقیقا چیست دارند: یک متخصص امنیت و متخصص IT ممکن است دید متفاوتی از کنترل کننده داشته باشند زیرا مستندات به صورت بدی نوشته شده اند. (منبع 7)  
یک نتیجه دیگر شکاف فرهنگی این است که پرسنل تاسیسات هسته ای معمولا در تشخیص دارایی حیاتی سایبریشان دشواری دارند. برای مثال در یک نیروگاه یکی از حیاتی ترین کنترل کننده ها -پمپی که برای بازگرداندن آب به درون نیروگاه بعد از رویداد از دست دادن آب استفاده می شود- دارای دکمه ای در اتاق کنترل بسیار امن بود اما PLC آن در یک ساختمان بود که نیازمند دسترسی با کارت بود اما یک محل حیاتی نبود. در ایالات متحده تلاشهای نوید دهنده ای اخیرا برای تشویق پرسنل نیروگاه هسته ای برای کار با پرسنل امنیت سایبری در جهت توافق در مورد اینکه کدام دارایی از نظر سایبری حیاتی هستند و باید برای حفاظت اولویت دار باشند انجام شده است اما تلاش های بیشتری مورد نیاز است.

تعاملات محدود

این مشکلات ارتباطس بین پرسنل نیروگاه هسته ای و پرسنل امنیت سایبری به دلیل تعاملات محدود بین دو گروه بزرگ‌تر هم می شوند. یک بخش مهم از چالش این است که افراد مسئول امنیت سایبری در تاسیات هسته ای در خود مکان حضور ندارند و در حقیقت در فاصله ی دوری ساکن هستند؛ بنابراین فرصت های محدودی برای تعامل حضوری پرسنل نیروگاه هسته ای و امنیت سایبری وجود دارد. علاوه بر این در میان گروه دومی مسئولیت به صورت زیادی پراکنده است. بنابراین برای بیشتر پرسنل نیروگاه هسته ای، ارتباط اصلیشان با مهندسان IT هنگامی است که گاهی اوقات برای انجام تعمیراتی به نیروگاه می آیند. هرچند احتمال اینکه این افراد همان افراد پاسخگوی رویداد سایبری باشند کم است.

هیچ نیروگاهی در کشور دارای متخصصان سایبری در محل نیست. من فکر می‌کنم آن‌ها مربوط به شرکت دیگری هستند و حتی در محل هم حضور ندارند. من هیچ ایده ای از اینکه آن‌ها که هستند نداشتم. فقط می‌دانستم که در دفتری در ۱۰۰ مایل دورتر حضور دارند (منبع ۶)

مشکلات آموزش

مشخص شده است که سطح و کیفیت آموزش امنیت سایبری در تأسیسات هسته ای در مقایسه با آموزش‌های لازم برای پرسنل هسته در سایر محل ها پایین است. مخصوصاً بعضی سازمان هایی که آموزش‌ها را انجام می‌دهند ممکن است متخصصان لازم را برای آن نداشته باشند. منبع ۲۳ می گوید:

بسیاری از شرکت ها جلسات آموزشی را ارایه می‌دهند اما تمام آن‌ها به یک اندازه توانایی ندارند. همیشه افراد درست آموزش‌ها را انجام نمی دهند. بسیاری از شرکت ها و بنیادها هنجارها را به کار می‌گیرند و می‌گویند که می‌توانند به مردم آموزش دهند بدون اینکه فرایند اعتبار سنجی وجود داشته باشد.

منبع ۶ می‌گوید که آموزش‌های او شامل مشاهده ی یک فیلم (که کاملاً هم آموزنده نبود) یک بار در سال، مشاهده ی مستندات رویه های امنیت سایبری و دادن یک امتحان بر اساس آن رویه ها است. به این‌گونه آموزش‌ها همچنین اشاره نمی‌کند که از دیدگاه امنیت سایبری چه روی می‌دهد و یا چگونه با پرسنل امنیت سایبری باید هماهنگ شد. این عدم کفایت آموزش به احتمال زیاد ناشی از دیدگاه صنعت هسته ای است که تهدیدات سایبری یک خطر جدی نیستند.

به طور خاص، به دلیل عدم وجود مانورها هیچ فرصتی برای تمرین رویه های رویداد امنیت سایبری برای پرسنل هسته ای ایجاد نمی‌شود و این یک مشکل است. در مقابل تأسیسات هسته ای مانورهای منظمی برای سایر سناریو ها دارند که شامل مانورهای مشترک با پرسنل امنیت فیزیکی برای آمادگی برای یورش های احتمالی است.

ناکافی بودن تمرینات به گونه‌ای است که هنگامی که پرسنل نیروگاه هسته ای در مورد رویه های امنیت سایبری آزموده می شوند، ممکن است سؤالات را به درستی درک نکنند و معمولاً رد می‌شوند در حالی که نتایج بالایی را در آزمون های مکرری که باید در مورد سایر رویه ها بدهند کسب می کنند.

یک روش واکنشی به جای یک روش فعال

یک نگرانی دیگر این است که امنیت سایبری در تأسیسات هسته ای واکنشی است تا فعال؛ به بیان دیگر تمرکز بر واکنش و پاسخگویی به رویدادها در هنگام وقوعشان است تا اینکه به صورت فعالانه به دنبال جلوگیری از حملات بود. در کل دفاع در تأسیسات هسته ای (مثلاً امنیت فیزیکی) وابسته به دریافت هشدار حمله قریب الوقوع است. برای نمونه اگر یک هواپیما به طرف یک تأسیسات هسته ای واقع در ایالات متحده در حرکت باشد اداره هوانوردی فدرال به تأسیسات برای اخطار به پرسنل آنجا خبر می دهد.

بسیاری از رویه ها برای واکنش به رویدادها در تأسیسات هسته ای بر اساس هشدار از یک تهدید قریب الوقوع یا از رویدادی است که واقع شده است….تماما واکنشی است، بر اساس اینکه یک نفر در تأسیسات می‌بیند که چیزی اتفاق افتاده است. (منبع ۶)

ما به مقدار زیادی واکنشی هستیم، چیزی در صنعت روی می‌دهد و ما از آن یاد می گیریم. می‌توانم به شما اطمینان دهم که آنچه در کره جنوبی در دسامبر ۲۰۱۴ روی داد می‌تواند باعث تغییرات زیادی در روشی شود که اپراتورها و کشورها در مورد امنیت سایبری فکر می کنند.

هرچند در هنگام یک حمله سایبری هیچ کدام از آن مکانیزم اخطارها وجود ندارد. در حقیقت همان‌طور که در بالا گفته شد،‌ یک تأسیسات هسته ای ممکن است تا هنگام وقوع از یک حمله سایبری مطلع نشود. برای نمونه،‌یک هکر می‌تواند یک بمب منطقی را وارد کند که تا هنگام فعال سازی برای ایجاد خسارت فیزیکی غیر فعال می ماند. در مورد تأسیسات هسته ای نطنز و بوشهر در ایران، پرسنل نیروگاه هسته ای می‌دانستند که سانتریفیوژهایشان در حال از هم پاشی است. هرچند در ماه های بعد بود که فهمیدند کرم استاکس نت عامل آن بوده است. به علاوه آسانی پنهان سازی کد مخرب باعث می‌شود که پیاده‌سازی چنان سیستم هشداری دشوارتر از سایر حوزه ها باشد و در مواردی ممکن است غیر ممکن باشد.

عدم آمادگی برای یک وضعیت اورژانسی امنیت سایبری با مقیاس وسیع

ترکیب عوامل گفته شده در بالا گویای این است که نیروگاه های هسته ای فاقد آمادگی برای یک وضعیت اورژانسی امنیت سایبری با مقیاس بالا هستند و باید مشکلات چشمگیری در تلاش برای هماهنگی سازی یک پاسخ مناسب وجود داشته باشد.

یک وضعیت اورژانسی امنیت سایبری با مقیاس بالا که در شب اتفاق بیافتد می‌توان بسیار خطرناک باشد. گیج‌کننده ترین زمان برای از سرویس خارج شدن یک سیستم در این زمان است. البته ممکن است که یک تیم آن کال که در حال انجام پویش برای ویروس و سایر بررسی ها وجود داشته باشند، اما این‌ها تنها تمهیدات پایه هستند و منبع ۶ توضیح می دهد:

هنگامی که ما می‌خواهیم افراد را در نیمه شب برای سایر مشکلات که به همان اندازه مهم هستند مانند خراب شدن یک پمپ فراخوانی کنیم،ِ پاسخگویی می‌تواند آهسته باشد. اگر شما افراد را در ساعت ۱ صبح فراخوانی کنید، چند دقیقه‌ای طول می‌کشد تا از خواب بیدار شوند. و شما نیاز به ۱۰ نفر دارید که آن کال باشند. زمانی که شما تمام افراد را در محل حاضر می‌کنید ممکن است بیشتر از یک ساعت گذشته باشد.

6. چالش های تکنیکی

خلاصه

این فصل تعدادی از چالش های تکنیکی مرتبط با تأمین امنیت سایبری در تأسیسات هسته ای را ارزیابی می کند. مهم‌تر از همه،‌ طراحی اولیه تأسیسات هسته ای-پیش از اینکه حملات سایبری یک نگرانی باشد- به این معنی است که از نظر طراحی نا امن هستند،‌ فاقد حفاظت های پایه شامل احراز هویت و رمزگذاری هستند. این بدین معناست که امنیت سایبری در تأسیسات هسته ای به مقدار زیادی وابسته به دفاع موفق از محیط پیرامون شبکه است – این دلیل است که انعطاف پذیری کد به معنای این است که هر حمله کننده ای که بتواند از دیوار دفاعی پیرامون عبور کند قادر یه انجام تغییرات منطقی در کد است به گونه‌ای که تقریباً غیرقابل دیدن است. علاوه بر این تعدادی تکنیک های امنیت سایبری مانند وصله کردن که در محیط IT خانه و دفتر استاندارد هستند،‌ در تأسیسات هسته ای به دشواری پیاده‌سازی می شوند. در آخر بی نهایت دشوار است که تمامیت زنجیره تأمین را تضمین کرد.

از نظر طراحی، غیر ایمن

یک چالش اصلی برای صنعت هسته ای، همان‌طور برای بیشتر زیرساخت های حیاتی، این است که معیارهای امنیت سایبری از ابتدا درون سیستم‌های کنترل صنعتی طراحی نشده اند. سیستم‌های کنترل درون بیشتر تأسیسات هسته ای در دهه 60 یا 70 میلادی هنگامی که کامپیوترها در دوره خردسالی بودند طراحی شده‌اند و طراحان هیچ فکری در مورد امکان اینکه یک فرد با یک انگیزه مخرب ممکن است به صورت عمدی سعی در حمله به یک سیستم کامپیوتری با استفاده از روش‌های الکترونیکی کند نکرده اند. به دلیل این پیش‌زمینه سیستم‌ها با در نظرگیری محافظت در برابر حملات سایبری طراحی و ساخته نشده‌اند و مقاوم سازی تمهیدات امنیت سایبری به این سیستم‌ها اکنون از نظر تکنیکی چالش برانگیز و هزینه بر است. منبع ۳ اظهار می کند:

یک جفت از ترفندهای کوچک در مورد اینکه شما دقیقاً در ابتدا در مورد یک سیستم چگونه فکر می‌کنید می‌تواند کاربرد عظیمی برای امنیت آن داشته باشد. اگر امنیت در مفهوم آن در نظر نگرفته شده باشد، دشوار است که بعداً به آن افزوده شود. در حقیقت نیازمند یک باز طراحی است.

یک مثال از طبیعت ٬از نظر طراحی، غیر ایمن٬ سیستم‌های کنترل صنعتی،‌ فقدان احراز هویت و تأیید است. به این صورت که ابزارهای موجود در محل، نیازمند احراز هویت نیستد که آیا فرمان فرستاده شده به آن‌ها یک فرمان معتبر است،‌یا اینکه تأیید کنند که از یک منبع درست آمده است. آن‌ها به گونه‌ای طراحی شده‌اند که بدون سؤال آنچه را که به آن‌ها گفته می‌شود انجام دهند. این یعنی هر حمله کننده ای که قادر به دسترسی باشد به راحتی می‌تواند فرمانی را به دستگاه بفرستد و آن هم انجام می شود. در نتیجه سیستم‌های کنترل صنعتی مخصوصا در برابر حملات فرد در میان (man-in-the-middle) که ارتباطات بین دو ابزار را مورد دستکاری قرار می‌دهد بی‌دفاع هستند:

دستگاه‌های در محل پیام را فوراً قبول می‌کنند بدون اینکه هیچ سؤالی کنند. دستگاه دریافت‌کننده نیاز به احراز هویت ندارد. سیستم‌های کنترل بنابراین به دلیل حملات فرد در میان ضعیف هستند. (منبع ۲۹)

شما می‌توانید به دستگاه‌های در محل هر چه دلتان می‌خواهد بگویید و آن‌ها هم به راحتی می پذیرند، ٬چشم، شما دستور دهید، من انجام می دهد٬. …. با مهارت ترین حمله کنندگان حتی به خودشان زحمت نمی‌دهند که آسیب‌پذیری ها را بیابند، آن‌ها تنها از امکانات موجود سیستم استفاده می کنند. (منبع ۱۳)

علاوه بر این انعطاف پذیری کد به این معنی است که یک حمله کننده می‌تواند منطق یا مجموعه ی دستورات برنامه‌ریزی را برای یک قسمت از تجهیزات با هدف اینکه به صورت متفاوتی رفتار کند تغییر دهد. این توسط کرم استاکس نت مورد سواستفاده قرار گرفت. تغییرات منطق به سختی شناسایی می‌شوند و بنابراین یک نگرانی اصلی هستند. در حالی که از نظر تکنیکی آزمایش کد برای تعیین اینکه آیا هیچ کدام از خطوط آن تغییر کرده است عملی است، در عمل این کار می‌تواند بسیار عظیم باشد زیرا یک سیستم عادی می‌تواند شامل میلیاردها خط کد باشند.

این دشواری به دلیل فقدان بررسی های سیستم‌های کنترل تشدید می شود. برای مثال آن‌ها معمولاً لاگ فایل‌هایی ندارند که موارد مانند اینکه کدام بخش از سیستم مورد دسترسی قرار گرفته، چه کسی آن‌ها را مورد دسترسی قرار داده است، کدام اطلاعات دیده شده است و در چه تاریخ و زمانی این عمل روی داده است را در خود ذخیره کند. بدون لاگ، تعیین اینکه یک هکر دسترسی پیدا کرد ه است و یا چیزی را تغییر داده است توسط متخصصان سایبر بسیار دشوارتر است.یک معنی اصلی وجود سیستم های ٬از نظر طراحی، غیر ایمن٬ این است که این سیستم‌ها کاملاً وابسته به سیستم دفاع شبکه پیرامونی هستن که از آن‌ها دفاع کنند، و عدم احراز هویت و انعطاف پذیری کد فرصتهایی را برای وارد آوری خسارات قابل توجه به تأسیسات فراهم می کند.

غیرممکن است که هنگامی که فردی به سستم دسترسی پیدا می‌کند از آن دفاع کرد. به این معناست که در حال حاضر ما کاملاً وابسته به دفاع پیرامونی هستیم تا هکرها را متوقف کنیم. (منبع ۱۳)

دشواری های وصله کردن

جنبه‌های منحصر به فرد محیطهای صنعتی (و مخصوصاً تأسیسات هسته ای) به این معنی است که تمهیدات امنیت سایبری استاندارد مورد استفاده درمحیط IT خانه یا دفتر الزاماً قابل استفاده نیست. متخصصان امنیت سایبری کاربران خانگی و دفتری را تشویق می‌کنند که وصله هایی را نصب کنند که آسیب‌پذیری های یافته شده در نرم‌افزار را برطرف می کند. با وجود این وصله کردن در نیروگاه هسته ای چالش های منحصر به فردی را ایجاد می‌کند و بنابراین به صورت مکرر مورد استفاده قرار نمی گیرد.

وصله کردن واقعاً چالش برانگیز است و واقعیت است است که افراد کمی وصله ها را نصب می کنند. (منبع ۳)

در ابتدا برخلاف محیط های IT خانه و دفتر معمولی، احتمال اینکه وصل ها برای سیستم‌های مورد استفاده در دسترس باشند کم است. بنابراین معمولاً سیستم‌های قدیمی وجود دارد که برای حداقل ۲۰ -۳۰ سال مورد استفاده قرار گرفته اند، برخلاف آن‌ها یی که در محیط خانه یا دفتر هستند، بسیاری از برنامه‌های این تأسیسات ها دیگر توسط تولید کننده پشتیباتی نمی شوند. تعدادی از تأسیسات سیستم‌های عامل MS-DOS یا Windows NT دارند که مایکروسافت دیگر برایشان وصله ارایه نمی‌دهد (و یا حداقل، نه با یک قیمت منطقی). در بعضی موارد تولید کننده ممکن است دیگر در بازار کسب و کار وجود نداشته باشد.

علاوه بر این وصله ها خطر خراب کردن سیستم‌هایی را که سعی در محافظتشان دارند ایجاد می کنند. یک وصله ممکن است با سایر برنامه‌ها یا سخت افزارهای یک سیستم سازگار نباشد یا ممکن است تأثیرات ناخواسته و یا دیده نشده داشته باشد. به دلیل اینکه اولویت اول حفظ در دسترس بودن نیروگاه است و یک وصله که مطابق انتظار کار نمی‌کند ممکن است کل یک نیروگاه را از کار بیاندازد بعضی از اپراتورها ریسک وصله کردن را بسیار بالا می‌بینند. منبع ۳ می گوید: من وصله هایی را دیده‌ام که سیستم‌ها را خراب کرده اند، جایی که به واقع سیستم را از کار انداخته اند. در محیط های خانه و دفتر نتایج، شدت کمتری دارند و معمولاً به سرعت قابل اصلاح هستند.

به دلیل اینکه اولویت اول حفظ در دسترس بودن نیروگاه است و یک وصله که مطابق انتظار کار نمی‌کند ممکن است کل یک نیروگاه را از کار بیاندازد بعضی از اپراتورها ریسک وصله کردن را بسیار بالا می‌بینند

حتی اگر یک وصله برای اجرا شدن در یک محصول تولید کننده آزمایش شده باشد، الزاما تضمین نمی‌کند که برای نصب ایمن است. تنها وجود یک بخش اضافی از نرم‌افزار مانند افزونه، در هنگام اجرا شدن در یک تأسیسات هسته ای میتواند یک ناسازگاری را با وصله ایجاد کند و سیستم را خراب کند. تولید کننده می‌تواند آزمایش کند که وصله در چندین حالت استاندارد ایمن است اما نمی‌تواند تمام ترکیب حالات ممکن را که نرم‌افزار می‌تواند در تأسیسات هسته ای اجرا شود آزمایش کند.

تنها به این دلیل که تولید کننده سیستم اتوماسیون شما یک وصله را تأیید کرده است، شما نمی‌دانید اکنون که افزونه های دیگری را در سیستم دارید آیا باز هم وصله تأثیر منفی ندارد. (منبع ۲۶)

خواص منحصر به فرد محیط های صنعتی مانند تأسیسات هسته ای به این معناست که حتی وصله کردن یک برنامه تجاری مربوط به شبکه ی درون تأسیسات می‌تواند نتایج چشمگیری داشته باشد. ممکن است در نظر گرفتن یک برنامه تجاری مربوط به شبکه درون تأسیسات به عنوان یک برنامه معمولی محیط IT دفتر منطقی به نظر بیاید و اینکه مشکل وصله ممکن است تنها شبکه را تحت تأثیر قرار دهد. با وجود این ارتباط درونی آن با سیستم‌های کنترل صنعتی به این معنی است که وجود مشکلی با یک وصله می‌تواند هردو سیستم را تحت تأثیر قرار دهد. همان‌طور که در جعبه ۱ گفته شد، در نیروگاه هسته ای هچ در جورجیا در سال 2008، یک وصله جهت هماهنگ سازی شبکه تجاری با شبکه سیستم کنترل صنعتی به کار گیری شد. متأسفانه وصله، داده‌های نادرستی را وارد سیستم کنترل صنعتی کرد و باعث خاموشی اتوماتیک نیروگاه شد.

به دلیل خطر خراب کردن سیستم توسط یک وصله، تأسیسات های هسته ای برخلاف محیط های عادی IT خانه و دفتر، باید وصله ها را پیش از نصب، به صورت کامل و به شدت آزمایش کنند. وصله هایی که سیستم‌های کلیدی را تحت تأثیر قرار می‌دهند نباید به دلیل خطر از کار انداختن کل نیروگاه به صورت مستقیم آزمایش و به کارگیری شوند. در عوض تأسیسات هسته ای معمولاً نیاز به راه اندازی یک سیستم هزینه بر کامل یا بخشی از آن جهت استفاده برای جایگزینی سیستم اصلی جهت بستر آزمون (test-bed) دارند.

{پاورقی۸: ساخت یک بستر آزمون برای یک تأسیسات هسته ای کاری مخصوصاً پیچیده است، زیرا سیستم‌های قدیمی شایع است. بسیاری از اجزای مورد استفاده در تأسیسات هسته ای دیگر تولید نمی شوند، بنابراین اپراتورها باید در بازارهای وسایل کهنه به دنبال آن‌ها بگردند. علاوه بر این تجهیزات باید کاملاً مشابه باشند تا یک وصله به صورت درستی آزمایش شود، زیرا تنها یک تفاوت در یک قطعه می‌تواند باعث شود که سیستم آزمون به صورت کاملاً متفاوتی رفتار کند. برای نمونه اگر یک کامپیوتر در یک تأسیسات هسته ای ویندوز ۹۸ را اجرا می‌کند در این صورت یک اپراتور باید یک کامپیوتر ویندوز ۹۸ که دقیقاً همان کارت گرافیک، کارت شبکه و سایر اجزای جهت بستر آزمون تهیه کند. در تهیه اجزا برای یک بستر آزمون چه برای یک سیستم قدیمی چه یک سیستم جدید، جایگزینی قطعات توسط تولید کننده قطعه می‌تواند مشکلات واقعی ایجاد کند. برای مثال اگر یک اپراتور در ژانویه یک کامپیوتر شخصی را بخرد و سپس دقیقاً همان مدل را در ماه مارس تهیه کند ممکن است که تولید کننده تعداد کمی از قطعات را در آن سه ماه تغییر داده باشد؛ حتی اگر دو کامپیوتر به نظر از یک مدل یکسان باشند از یک تولید کننده باشند، ممکن است کاملاً یکسان نباشند. با این وجود حتی اختلافات کوچک مانند این‌ها می‌تواند باعث شود که سیستم آزمایشی در یک حالت متفاوت رفتار کند.}

داشتن یک سیستم آزمایشی بسیار گران قیمت است. و حتی در این صورت شما هیچ وقت دو راکتور هسته ای کاملاً مشابه ندارید. با وجود این برای داشتن یک آزمون کاملاً دقیق ممکن است نیاز به مدلی دقیقاً یکسان داشته باشید. (منبع ۹)

حتی اگر یک وصله در دسترس باشد و مورد آزمایش قرار گرفته باشد، یافتن یک پنجره زمانی که در آن به کارگیری شود معمولاً دشوار است. تأسیسات هسته ای ۲۴ ساعته در روز کار می‌کنند اما نیروگاه برای اعمال وصله ها باید خاموش شود مخصوصاً اگر سیستم‌های کلیدی را تحت تأثیر قرار دهند. بعضی از سیستم‌ها این توانایی اساسی را برای ادامه به کار تأسیسات حتی اگر آن‌ها را به صورت موقت از خدمت خارج کرد ارایه می‌دهد اما این کار باعث نقض عمل‌کرد ایمن نیروگاه می شود. نیروگاه های برق هسته ای ممکن است به صورت خاص برای تعمیر و نگهداری هر دو سال یک بار خاموش شوند بنابراین نصب یک وصله ممکن است تا زمان یک خاموشی از پیش برنامه‌ریزی شده ممکن نباشد. دوباره این برخلاف تمام محیط های IT خانگی و دفتری است که وصله ها می‌توانند در زمان بیکاری نصب شوند.

شما مجبورید که مطمین شوید که حتی یک پنجره تغییر دارید. اکنون اگر شما یک پنجره تغییر داشته باشید در این صورت احتمالاً سازمان ها خودشان باید عملیات را به صورت موقت متوقف کنند، شما در مورد یک عملیات ۲۴/۷ صحبت می کنید. (منبع ۳)

به دلیل اینکه وصله کردن در یک نیروگاه هسته ای تنظیمات یک سیستم را تغییر می‌دهد، بررسی سیستم را برای هر رفتار غیر طبیعی که ممکن است نشان دهنده ی آلودگی توسط یک بدافزار باشد را دشوار تر می کند. میان اپراتورهای هسته ای، گرایش این است که از تغییرات یک سیستم خودداری کنند تا اینکه اپراتوربتواند یک دید عمیق از چگونگی کار سیستم به دست بیاورد؛ در لحظه‌ای که یک وصله نصب می شود، یک سیستم تغییر می‌کند و اپراتور آن عمق از درک را از رفتار سیستم ندارد. وصله کردن به این دلیل به صورت چشمگیری کارایی تکنیک های نظارت را که به دنبال ناهنجاری رفتاری است، می کاهد. اما دوباره این در تضاد کامل با تغییرات تنظیمات سیستم در محیط های IT خانگی و دفتری است که به صورت مداوم تغییر می کنند (و وصله می شوند ).

حالت پیشفرض این است که همان‌طور که شما یک سیستم را توسعه و آزمایش می کنید، به همان صورت باقی می ماند. اپراتورهای صنعتی این کار را انجام می‌دهند زیرا کار می کند. هر تغییری که شما انجام می‌دهید عدم قطعیت هایی را وارد می‌کند و همیشه هم همین‌طور است. (منبع ۹)

در نهایت وصله کردن یک چرخه بی پایان است زیرا به صورت مرتب آسیب‌پذیری های جدیدی کشف می‌شوند و همراه با آن‌ها نیاز به یک وصله جدید احساس می شود.

شما می‌توانید تمام این زمان را صرف وصله کردن سیستمتان بکنید و فردا به همان اندازه کهنه و از مد افتاده خواهند بود که قبل از اینکه شما وصله کنید بودند. (منبع ۲۷)

این چالش به دلیل تعداد بالای سیستم‌هایی که نیاز به وصله شدن در یک تأسیسات هسته ای دارند بزرگ‌تر هم می شود. برای اینکه وصله کردن مؤثر باشد، یک اپراتور با این نیاز روبه رو می‌شود که هر تک وسیله‌ای در آن تأسیسات باید به صورت مرتب وصله شود اما همواره یک زمان چشمگیر میان کشف یک آسیب‌پذیری و تا اینکه تولید کننده یک وصله را توسعه دهد و آن را آزمایش کند وجود دارد که سیستم آسیب‌پذیر است. این فرایند در بهترین حالت می‌تواند هفته‌ها و ماه ها به طول بیانجامد اما در بسیاری از حالات می‌تواند سالها طول بکشد.

برای محدود کردن در معرض خطر قرار گیریتان، شما باید همه چیز را وصله کنید. شما باید سویچهایتان را وصله کنید، شما باید دیوار آتشهایتان را وصله کنید، شما باید ابزارهای توکارتان را وصله کنید. (منبع ۲۷)

به این صورت به نظر می‌آید که هر تأسیسات هسته ای باید به صورت دقیقی مزایا و معایب وصله کردن را در هر مورد ارزیابی کند. بسیاری به نظر می‌آید که خطر را بیشتر از منافع دانسته و تصمیم به وصله نکردن گرفته اند.

چالش های زنجیره تأمین

آسیب‌پذیری های زنجیره تأمین یک نگرانی در حال رشد است زیرا تجهیزات استفاده شده در یک تأسیسات هسته ای (و به صورت عام‌تر در زیرساخت های حیاتی) می‌توانند در هر مرحله‌ای در معرض خطر قرار گیرند. دسترسی به در پشتی یا سوء‌استفاده ها می‌تواند ایجاد شود برای نمونه در تأسیسات تولید کننده،‌هنگامی که تجهیزات در حال طراحی و سرهم بندی است، یا در مراحل مربوط به پیمان کاران فرعی. به دلایل صرفه هزینه ای، تولید کنندگان تمایل به استفاده از زیر قطعات متعلق به منابع دیگر دارند شامل آن‌ها یی که در سایر کشورها تولید شده است. حتی فاز حمل و نقل هم آبستن سوء‌استفاده است. فاش سازی های اسنودن{پاورقی ۹: در ماه می ۲۰۱۳ مامور سابق NSA، ادوراد اسنودن ده‌ها هزار سند حساس و طبقه بندی شده را که شامل فعالیت‌های جاسوسی هدایت شده توسط ایالات متحده است فاش کرد} شواهدی را ارایه کرد که آزانس امنیت ملی ایالات متحده (NSA) مسیریاب ها و سایر ابزارهای شبکه ای را ره گیری کرده است که به خارج صادر می‌شوند و درهای پشتی یا راه‌های برای به دست آوردن دسترسی از راه دور بدون اجازه را به سیستم‌های کامپیوتری فراهم می‌کند (Greenwald, 2014) منبع ۲۸ می گوید:

ما واقعاً هیچ راهی نداریم که در برابر خطرات زنچیره تأمین در یک موقعیت استفاده از تسلیحات جنگ سایبری از خود دفاع کنیم: یک کامپیوتر یا سیستم می‌تواند در هنگام انتقال یا در محل تولید مورد دستکاری قرار گرفته باشد.

هرچند تهدیدات زنجیره تأمین در حال حاضر به صورت عام محدود به تعداد کمی از عامل های ایالتی هستند که تلاش می‌کنند تا منطقه را برای یک سناریوی منازعه سایبری آماده کنند، ممکن است که گروه‌های تروریست و یا حتی هکر ها هم بتوانند از آن تاکتیک‌ها اقتباس کنند.

البته سازمان های اطلاعاتی تمام دنیا نگران این آسیب‌پذیری ها هستند -بخصوص در هنگام افشاگری اسنودن- و تعدادی از کشورها به صورت فزاینده ای به دنبال ملی کردن زنجیره تامینشان هستند. هرچند واقعیت جهان شدن این است که تعداد کمی از کشورها قادر به تولید تمام بخش‌های مورد نیاز برای یک نیروگاه هسته ای هستند. براساس گفته‌های منبع ۵:

ایالات متحده می‌خواهد که آن را انجام دهد(تولید تمام قطعاتش)ُ ، اما من فکر نمی‌کنم که دیگر بتواند آن را انجام دهد. من فکر نمی‌کنم یک نفر در یک موقعیت بتواند آن را انجام دهد.

برای نمونه، تنها یک کامپیوتر استفاده شده در یک تأسیسات هسته ای شامل هزاران قسمت است. در میان این‌ها، تقریباً اجتناب‌ناپذیر است که ممکن است یک چیپ کوچک وجود داشته باشد که در تایوان تولید شده باشد و یا سایر زیر قطعات خارجی وجود داشته باشد.

۷. برخورد با چالش ها: راه پیش رو

خلاصه

برخورد با چالش های توضیح داده شده در فصل های قبلی نیازمند ترکیبی از سیاست و تمهیدات تکنیکی است. این فصل یک سری از راه حل‌هایی را ارایه می‌دهد که در اطراف چندین موضوع متمرکز شده اند. فرای همه نیازی برای دستورالعمل های ارزیابی خطر بهسازی شده در مورد امنیت سایبری در تأسیسات هسته ای وجود دارد که بتواند یک زیربنای محکم اقتصادی را برای سرمایه‌گذاری فراهم کند. عامل انسانی می‌تواند در طول یک مجموعه از ارتباطات بهتر در مورد خطرات بهداشت سایبری ضعیف، و تمهیدات مقاوم سازی قویتر مدیریت شود.

بهتر کردن انتشار و به اشتراک گذاری اطلاعات می‌تواند با تشویق به اشتراک گذاری ناشناس، پرورش ارتباط فردی در کنفرانس های بین‌المللی و تاسیس CERT های صنعتی به دست آید. همچنین نیاز به استانداردهای تنظیمی و تامنی مالی بیشتر برای آژانسهای مانند IAEA وجود دارد. شکاف فرهنگی می‌تواند با تمهیداتی مانند تشویق مهندسان IT برای دیدن نیروگاه های هسته ای، برنامه‌های آموزشی بین رشته ای و بهتر کردن آموزش امنیت سایبری پر شود.

تمهیدات تکنیکی مانند خودداری از استفاده از امکانات دیجیتال غیر ضروری، پیاده‌سازی تکنولوژی های لیست سفید (مجوزدهی)، نظارت بر شبکه و تشویق به اقتباس از دیودهای داده‌ای، همه می‌توانند امنیت سایبری را بهبود بخشند. کشورها می‌توانند خطر زنجیره تأمین را با کاهش وابستگیشان به اجزای خارجی به حداقل برسانند.

ارزیابی خطر – و جذب سرمایه

با دانستن اینکه باور غالب در صنعت هسته ای این است که امنیت سایبری نمی‌تواند یک خطر حقیقی را برای تأسیسات هسته ای ایجاد کند، قدم اول این است که آگاهی از این چالش را افزایش داد. یک راه برای انجام آن می‌تواند به وسیله ی توسعه دستورالعمل هایی در مورد راه‌های اندازه‌گیری خطرات امنیت سایبری در صنعت هسته ای است. به دلیل اینکه در حال حاضر هیچ نوع روش ارزیابی خطری وجود ندارد که به یک تأسیسات هسته ای اجازه ی اجرای یک ارزیابی خطر امنیتی و خطر ایمنی مرکب (تنها یک ارزیابی خطر ایمنی و یک ارزیابی خطر امنیتی جداگانه که شامل خطر امنیت سایبری است) را بدهد، آن دستورالعمل ها شامل نیاز برای روشهای ارزیابی خطر مرکب برای ایمنی و امنیت هستند. توسعه ی یک روش نیازمند انعکاس درون صنعت است که احتمالاً توسط گروه رابط IAEA، که برای پرداختن به اولویت های در تناقض بین ایمنی و امنیت ایجاد شده است هدایت می شود

یک فهم بیشتر از خطر همچنین در برخورد با چالش پرداختن ناکافی به امنیت سایبری در صنعت کمک می کند. به علاوه ایجاد آگاهی از نیاز به سرمایه‌گذاری در امنیت سایبری، امنیت سایبری را از نظر تجاری جذاب‌تر می‌کند و یک منطق اقتصادی روشن را برای مدیران عامل و هیئت مدیره ی شرکت های بزرگ در افزایش سرمایه‌گذاری در این موضوع را فراهم می کند.

به دلیل اینکه صنعت بیمه نیازمند ارزیابی خطر جدی است، توسعه بیشتر و اقتباس بیمه سایبری در بخش هسته ای ممکن است در توسعه این دستورالعمل ها برای اندازه‌گیری خطر سایبری یاری رسان باشد؛ بنابراین بیمه سایبری می‌تواند یک ابزار مهم برای افزایش امنیت سایبری باشد. دولت فرانسه یک مطالعه عظیمی را در مورد این سؤال انجام می دهد. یک نتیجه‌گیری اولیه این است که برای موفقیت (و برای یافتن سطح درست در معرض خطر قرارگیری بیمه گر در هنگام محاسبه در برابر خطر امنیت سایبری)، یک نیاز کلیدی محاسبه ی دقیق آن خطر بر اساس معیارهای مشترک بین بیمه شونده و بیمه گر است.

چیزی که بیمه گر نیاز دارد، فهم از خطر است و آن هم بستگی به این دارد که آیا سازمان ها افراد درست را در جای درست دارند که مسئولیت های درست برای انجام تصمیمات درست داشته باشند و آیا سیاست درست و ساختار عملیاتی در جای خود دارند؟

همچنین بیمه ممکن است نیازمند جذاب سازی تجاری بیشتر امنیت سایبری و هدایت فرایند پیاده‌سازی تمهیدات مناسب با تأمین انگیزه مالی مورد نیاز(به شکل حق بیمه کمتر) برای قانع کردن دارنده-اپراتور در سرمایه‌گذاری در آن‌ها باشد.

اگر یک شرکت بیمه به یک دارنده-اپراتور بگوید که حق بیمه آن‌ها بسیار بالاست زیرا آن‌ها تمهیدات امنیت سایبری کافی ندارند، دارنده-اپراتور ممکن است به این صورت نتیجه‌گیری کند که ٬اگر من ۱۰۰۰۰۰ دلار را برای تمهیدات امنیت سایبری خرج کنم می‌توانم ۲۰۰۰۰۰ را در حق بیمه صرفه جویی کنم٬ . (منبع ۱۰)

کنترل عامل انسانی

با دانستن اینکه بخشی از چالش نشئت گرفته از عامل انسانی ـمانند مهندسان یا ماموران که روابط بدون اجازه و سرکشانه ایجاد می‌کنند و یا آن‌هایی که لپتاپ خانگیشان را به صورت مستقیم درون شبکه تأسیسات هسته ای وارد می کنندـ است، ایجاد آگاهی درون پرسنل درگیر در مورد خطرات ایجاد شده در عمل‌کرد به آن صورت، کلیدی خواهد بود.

همچنین نیاز است تا تأسیسات هسته ای قوانینی را که تاکنون وجود نداشته است وضع کنند. برای نمونه در کشورها یا تاسیساتی که وسایل شخصی درون تأسیسات هسته ای به صورت علنی ممنوع نیست، مهندسان باید مجبور شوند که هر نوع از وسایل شخصی مانند لپتاپ را در هنگام ورود به تأسیسات تحوسل دهند؛ وسایل تنها در هنگام خروج به آن‌ها تحویل می شود.

مهندسان باید مجبور شوند که هر لپتاپ شخصی را که به نیروگاه می‌آورند تحویل دهند. (منبع ۷)

اگر شما می‌خواهید هر نوع آزمایشی انجام دهید و هر نوع از وسایل شخصی را همراه دارید، باید آن را تحویل دهید و ما هنگامی که لپتاپتان را تحویل می‌دهید آن را به شما بر می گردانیم. (منبع ۶)

همچنین نیاز به قوانینی وجود دارد که پرسنل نیروگاه هسته ای را مجبور کند تا رمز پیشفرض موجود در دستگاه ها را به یک زمر ایمن تغییر دهند؛ این باید به هر دو نوع تجهیزات حاضر و هر تجهیزات جدیدی که نصب می‌شود اعمال شود.

برای اطمینان از اینکه مهندسان در عمل این سیاست‌ها را دنبال می کنند، اجبار ضروری است. مخصوصاً روشهای تأیید مستقل که در آن‌ها انطباق با رویه ها را بررسی می‌کنند باید در موارد سایبری با قدرت دنبال شود. منبع ۶ می‌گوید که اگر یک ابزار تحویل داده شد قبل از اتصال با نیروگاه هسته ای یک فرد مسئول باید به صورت مستقل ارزیابی کند که ابزار مورد نظر درست است؛ یک فرد دیگر هم باید مسئول بررسی ویروس برای وسیله باشد.

همچنین روشهای تکنیکی می‌تواند برای اعمال اانطباق با قوانین مورد استفاده قرار گیرد. برای نمونه با دانستن اینکه پرسنل نیروگاه هسته ای ممکن است ابزارهای USB را حتی با وجود ممنوع بودن وارد کامپیوترهای تأسیسات هسته ای کنند، مالک-اپراتورها ممکن است نیاز به چسب کردن پورت های USB داشته باشند.

افرادی که در نیروگاه های هسته ای کار می‌کنند ممکن است نسبت به یک محیط استاندارد IT بیشتر علاقه‌مند کار کردن با پورت های چسب شده باشند. پورت های چسب شده در یک اتاق نیروگاه به احتمال زیاد بهره وری را تحت تأثیر قرار نمی دهند؛ تنها شارژ یک ایفون را سخت تر می کنند. از طرف دیگر پورت های USB چسب شده در یک محیط IT قطعاً اثربخشی کارمندان را تحت تأثیر قرار می دهند (منبع ۲۶)

یک گزینه ی دیگر این است مطمین شویم ابزارهای usb قبل از اجازه ی ورود به درون تأسیسات از نظر بدافزارها بررسی و پاکسازی شده اند. یک شرکت تکنولوژی را برای انجام آن توسعه داده است.

یک شرکت در جنوب فرانسه وجود دارد که تکنولوژی را توسعه داده است که ابزارهای پاکسازی USB را ایجاد می کند. بنابراین ما نمی‌گوییم که USB تان را سر کار نیاورید بلکه حداقل می‌توانیم آن USB را به ابزاری مخصوص وصل کنیم که تمام داده‌های موجود بر روی آن را آزمایش می کند، فایل‌هایی را که قابل اجرا شدن هستند اجرا می‌کند و قبل از اینکه فرد آن ابزار USB را مستقیماً به درون یک وسیله حساس وارد کند مطمین می‌شود که هیچ بدافزاری بر روی آن‌ها نیست. (منبع ۲۶)

ترویج افشا و به اشتراک گذاری اطلاعات

به دلیل اینکه بی میلی صنعت در به اشتراک گذاری اطلاعات در مورد حملات سایبری رخ داده ناشی از نگرانی‌هایی در مورد آسیب احتمالی به اعتبار آنهاست، تشویق تأسیسات هسته ای برای به اشتراک گذاری اطلاعات تهدیدها به صورت ناشناس می‌تواند کمک به افشای بیشتر اطلاعات شود. ناشناسی می‌تواند به این صورت به دست آید که از تأسیسات بخواهیم ٬شاخص های دستکاری٬ را به اشتراک بگذارند؛ اینها نشانه‌های باقی‌مانده در شبکه یا سیستم است که نشان دهنده ی این است که یک عامل مخرب در سیستم وجود داشته است. این‌ها ممکن است شامل ایمیل‌های فیشینگ (phishing) یا خود کد مخرب باشد. در به اشتراک گذاری شاخص های دستکاری، تأسیسات هسته ای نه مجبور هستند هویتشان را فاش کنند و نه اینکه تأثیرات حمله چه بوده است.

به اشتراک گذاری شاخص های دستکاری می‌تواند کل صنعت را کمک کند و امنیت را بهتر کند. ما می‌توانیم به صورت ناشناس شاخص های دستکاری را بدون دانستن اینکه چه کسی مورد حمله قرار گرفته است به اشتراک بگذاریم. (منبع ۲۶)

با دانستن اینکه تأسیسات هسته ای تمایل به تمرکز بر واکنش به حملات در هنگام وقوع دارند، یک مزیت به اشتراک گذاری شاخص های دستکاری این است که باعث ایجاد یک روش فعالانه برای جلوگیری از حملات می شود. در نقل و انتقال اطلاعات باارزش در مورد جلوگیری از حملات -شامل انواع آسیب‌پذیری ها مورد سو استفاده قرار گرفته توسط هکرها، مسیرهای حمله استفاده شده برای به دست آوردن دسترسی و سیستم‌های هدف- به اشتراک گذاری شاخص های دستکاری می‌تواند به بقیه کمک کند تا خیلی زود از خطر احتمالی خبردار شوند. این می‌تواند آن‌ها را قادر سازد که تمهیداتی دفاعی را ایجاد کنند، احتمالاً با افزایش نظارت یا با تصمیم در مورد وصله زنی به سیستم‌هایی که به عنوان آسیب‌پذیر شناخته شده اند.

به اشتراک گذاری ناشناس در سایر حوزه ها هم موفق بوده است. همان‌طور که منبع ۵ گفته است:

صنعت هوانوردی یک زیرساخت را برای اینکه خلبان‌ها و سایر پرسنل حاضر در صنعت بتوانند به صورت ناشناس حوادث را گزارش کنند ایجاد کرد (برای نمونه اگر دو هواپیما خیلی به هم نزدیک شده اند)؛ این روش باعث افزایش افشای اطلاعات و ایمنی صنعت شد. اینگونه مکانیزم ها می‌تواند در صنعت هسته ای و همچنین در بخش صنعتی به صورت عامتری کپی و اقتباس شود.

کمک به ارتباط فردی، که در ایجاد اعتماد ضروری برای به اشتراک گذاری اطلاعات، الزامی است، همچنین کلیدی برای ارتقای مبادله ی اطلاعات در هر دو سطح ملی و بین‌المللی است. افراد ممکن است به سایر شرکت ها اعتماد نداشته باشند -یا در این مورد دولتها- اما آن‌ها به سایر افرادی که با آن‌ها ارتباطات قوی فردی برقرار کرده‌اند اعتماد دارند؛ بنابراین آماده اند که خطر به اشتراک گذاری اطلاعات را بپذیرند. کنفرانس های بین‌المللی می‌توانند یک مسیر برای ایجاد این ارتباطات باشند و تلاش‌های مانند آن، در صنعت هسته ای (و به صورت عامتر هر زیرساخت حیاتی) باید تشویق شوند.

ارتباطات فردی همیشه برای اشتراک اطلاعات بهترین راه حل هستند؛ این محیط های مورد اعتماد در حالتی به بهترین صورت موثرند که آن‌ها نخواهند در یک سناریوی جنگ سایبری به همدیگر حمله کنند. تعداد زیادی نیروگاه هسته ای در جهان وجود ندارد بنابراین پیاده‌سازی این کار ممکن است؛ نیاز به یک حس همکاری وجود دارد. (منبع ۱۱)

هرچند دولت ها نگرانند که اشتراک اطلاعات تهدید با سایر دولتها می‌تواند امنیت ملی را به خطر بیاندازد و برای همکاری در سطح بین‌المللی بی میلند، با وجود این درک کرده‌اند که این اشتراک در سطح ملی یک مزیت کلیدی برای دفاع است. دولتها بنابراین می‌توانند یک نقش کلیدی در ترویج به اشتراک گذاری اطلاعات درون کشورهای خودشان با کمک به تاسیس گروه پاسخ اضطراری کامپیوتری که در سیستم‌های کنترل صنعتی تخصص دارند، ایفا کنند.

مشخصات منحصر به فرد سیستم‌های کنترل صنعتی به این معناست که اهتمام ویژه CERT به سیستم‌های کنترل صنعتی مؤثرتر خواهد بود. در حقیقت ایالات متحده در سیستم‌های کنترل صنعتی که CERT (یا ICS-CERT) در سال ۲۰۰۹ راه اندازی کرده است موفق عمل کرده است؛ این سیستم‌ها به علاوه ی CERT ملی (که US-CERT خوانده می شود) در حال عملیات هستند. البته برای کشورهایی که هنوز موفق به ایجاد CERT خودشان نشده اند، ایجاد آن اولویت اول است و ICS می‌تواند به عنوان یک بخش از این کار تحت عنوان مرحله اول به کارگیری شود.

تنظیم کننده ها باید بفهمند که برای پرورش یک فرهنگ امنیت سایبری فعالانه تر، باید راضی شوند که از بعضی از مکالمات ضروری بین ذینفعان دور بمانند.

تا اندازه‌ای از به اشتراک گذاری بین‌المللی با حمایت دولت می‌تواند بین متحدان نزدیک به وقوع بپیوندد. یک راه برای این CERT های ملی هستند؛ ترویج اشتراک اطلاعات بیشتر بین CERT های ملی می‌تواند پرمنفعت باشد. در حال حاضر تنها یک اشتراک محدود بین CERT ها به یک شیوه ی غیر رسمی و موردی وجود دارد (منابع ۱۹-۲۲). حتی با وجود اینکه بعضی از دولت ها نسبت به اطلاعاتی که می‌دهند اطلاعات بیشتری می گیرند، این کار هم باعث تقویت امنیت سایبری می شود. بسیاری در صنعت احساس می‌کنند که هر به اشتراک گذاری اطلاعات، هر چند محدود هنوز هم بهتر از وضعیت حداقلی موجود است.

داشتن اشتراک اطلاعات بیشتر بین CERT ها می‌تواند یاری رسان باشد. البته بیشتر کشورها می‌خواهند که اطلاعات بگیرند تا اینکه اطلاعات بدهند. اما اگر شما به کشورها اجازه دهید که آنچه را می‌خواهند بدهند و آنچه را که می‌خواهند بگیرند ایده‌آل نیست اما از آنچه که ما امروزه داریم بسیار بهتر است چون امروزه ما هیچ چیز نداریم. (منبع ۲۵)

علاوه بر این با دانستن اینکه دارنده-اپراتور می‌تواند از افشای حملات امنیت سایبری یا رویدادهایی که آن‌ها مسئولند آگاه باشد، این محیطی را می‌سازد که آن‌ها احساس می‌کنند که می‌توانند به صورت داوطلبانه بدون ترس از پیامدهای آن صحبت کنند و این کلیدی برای افزایش سطح گزارش‌ها به ICS-CERT ها (یا به صورت گسترده‌تر CERT ها) است. تنظیم کننده باید به دارنده-اپراتور اطمینان دهد که آن‌ها برای هیچ کدام از اطلاعاتی که به اشتراک می‌گذارند -به شرطی که اعتماد خوبی نشان دهند- مجازات نخواهند شد و اینکه اگر آن‌ها یک مشکل یا رویداد امنیت سایبری را که به دلیل اجرا نکردن دستورالعمل پیش آمده است افشا کنند آن‌ها تحت پیگرد قرار نمی گیرند. براساس منبع ۲۰: برای ایجاد اشتراک گذاری اطلاعات، شما باید فرهنگی را ایجاد کنید که هر آنچه که شما می‌گویید علیه شما به کار گرفته نمی شود.

به این ترتیب تنظیم کنندگان نیاز به درک این دارند که برای پرورش یک فرهنگ امنیت سایبری فعالانه تر در بخش هسته ای، آن‌ها باید خود را ملزم به دوری از بعضی از مکالمات ضروری بین ذینفعان کنند، و تمرکز اصلی آن‌ها بر نتیجه باشد تا اینکه بر مکانیک های ارایه یک سطح حداقل از امنیت. آن‌ها همچنین باید از دشواری های امنیت در رسانه ی الکترونیک آگاه باشند و یک روش عملی را برای اجرای قوانین انتخاب کنند. هر سیستم چه اینکه دارای شکاف هوا باشد، وصله شده باشد و به هر روشی محافظت شده باشد، امکان نفوذ دارد؛ تا زمانی که دلیل ریشه‌ای یک حمله ی خاص، مشخصاً تخلف عمدی و غیرعمدی از قواعد نباشد، تنظیم کنندگان تنها باید نگران این باشند که بخش هسته ای باید در همان حال که فرهنگ امنیت سایبری در طول زمان رشد می‌کند و قابلیت‌های مرتبط توسعه می یابد، از تجربیاتش یاد بگیرد.

توسعه ی تمهیدات امنت بین‌المللی

تعدادی از تمهیدات سیاسی هم می‌تواند مفید باشد. با دانستن اینکه فقط تعداد کمی از ملت‌ها دستورالعمل هایی در ارتباط با امنیت سایبری در تأسیسات هسته ای دارند، سایر کشورها هم باید برای اقتباس استاندارد های مربوط به دستورالعمل تشویق شوند. به دلیل اینکه تعداد زیادی از کشورها تابع دستورالعمل های IAEA هستند، توسعه بیشتر کارهای آژانس در مورد امنیت سایبری در تأسیسات هسته ای می‌تواند مفید باشد. این می‌تواند با تخصیص منابع بیشتر به IAEA (وسایر آژانس ها) برای قادر کردن آن‌ها جهت برخورد موثرتر با تهدیدات امنیت سایبری می‌تواند انجام شود.

توجه ویژه ای باید به کمک به کشورهای در حال توسعه جهت افزایش آمادگیشان برای امنیت سایبری در بخش هسته ای تخصیص یابد زیرا آن‌ها بیشتر در برابر حملات آسیب پذیرند. این کشورها احتمالاً نیاز به کمک مالی هم برای انجام این کار دارند.

پر کردن شکاف های ارتباطی

برای غلبه بر موانع ارتباطی بین پرسنل نیروگاه هسته ای (مهندسان OT) و پرسنل امنیت سایبری (مهندسان IT)، پرورش ارتباطات چهره به جهره بین دو گروه ضروری است. برای مثال مهم است که پرسنل امنیت سایبری به صورت فیزیکی و طبق برنامه مرتب تأسیسات هسته ای را ببینند. به دلیل تمهیدات صرفه جویی در هزینه، آن‌ها مجبورند که از روش‌های همکاری از راه دور استفاده کنند اما ارتباط چهره به چهره کلیدی است برای ارتقای درک دوطرفه بین دو فرهنگ. مخصوصاً تشویق پرسنل نیروگاه هسته ای و پرسنل امنیت سایبری برای کار با همدیگر بر پروژه های مشترک به آن‌ها اجازه می‌دهد که درک بیشتری از طرز فکر همدیگر به دست بیاورند. این ممکن است برای مثال شامل کار با همدیگر بر روی تحلیل مشترک آسیب‌پذیری و یا ارزیابی خطر باشد. این ممکن است به ایجاد آگاهی کلی از خطرات امنیت سایبری میان پرسنل نیروگاه هسته ای کمک کند.

در حقیقت مجبور کردن فرد IT برای کار در نیروگاه، نشستن با مهندسان و کار با آن‌ها و انجام کارها در محیط های OT روشی است که شما مطمین می‌شوید OT و IT همدیگر را درک می کنند. (منبع ۲۶)

شما نیازمند یک متخصص IT هستید که با یک متخصص امنیت درون نیروگاه صحبت می‌کند تا اینکه آن‌ها بتوانند زبان مشترکی را بفهمند. (منبع ۷)

مهم است که کیفیت تمرینات امنیت سایبری را در تأسیسات هسته ای افزایش داد. با دانستن اینکه یک مشکل مشخص شده این است که بعضی از تمرینات ممکن است توسط گروهی بدون صلاحیت کافی انجام شود، نیاز به اعتبار سنجی برنامه‌های تمرینی وجود دارد. منبع ۲۴ پیشنهاد می‌دهد که IAEA کسی باشد که بتواند اعتبارسنجی بین‌المللی را فراهم کند.

به علاوه کیفیت تمرینات و دفعات آن‌ها می‌تواند با برگزاری مانورهای یکپارچه به صورت مرتب افزایش یابد. این همچنین یک مسیر یکپارچه برای ارتباط بین دو گروه ایجاد می‌کند و اختلاف فرهنگی را کاهش می دهد.

همچنین یک نیاز فوری برای دانشگاه‌ها و برنامه‌های تخصصی میان رشته ای وجود دارد. برنامه‌های میان رشته ای در امنیت سایبری سیستم‌های کنترل صنعتی درون صنعت هسته ای که شامل رشته‌های علوم کامپیوتر و مهندسی است در حال تاسیس شدند هستند و خلق تعداد بیشتری از این برنامه‌ها باید باهدف کمک به پر کردن شکاف های فرهنگی و شروع به ایجاد تغییرات فرهنگی درون صنعت تشویق شود. (IAEA, 2014a)

تلاشی دیگر برای بهتر کردن ارتباط با توجه به مکالمات محدود بین شرکت های امنیت سایبری و تولید کنندگان، این است که مشارکت بین متخصصان امنیت سایبری و تولید کنندگان افزایش یابد. درک عمیقتر از اینکه چگونه پروتکل های تناسب تولیدکنندگان کار می کند، شرکت های امنیت سایبری را قادر می‌سازد که محافظت های امنیتی بیشتری را برای این محصولات فراهم کنند. براساس گفته‌های منبع ۲۵، شرکت امنیت سایبری McAfee اخیراً قرارداد مشارکت با تولیدکنندگانی مانند Alstom و Schneider را برای رسیدن به این هدف امضا کرده است.

افزایش امنیت

با دانستن اینکه بیشتر سیستم‌های کنترل صنعتی بدون در نظر گرفتن نیازهای امنیت سایبری ـ و همان‌طور که در بالا گفته شد اضافه کردن افزونه های امنیت سایبری بعداً دشوار است- ضروری است که طراحان نسل آینده سیستم‌های کنترل امنیت سایبری را در طول فاز مفهومی اولیه در نظر داشته باشند. برای مثال ICS باید از وارد کردن امکانات دیجیتالی غیرضروری که می‌تواند نقطه ضعف‌های امنیت سایبری ایجاد کند خودداری کند؛ در غیر این صورت حذف این امکانات نیازمند بازطراحی کامل یا جزئی است. در عمل این بدین معناست که کارایی های بسیار مهم نباید دیجیتالی سازی شوند.

دوتا از ترفندهای کوچک در مورد چگونگی درک شما از یک سیستم، درست در اولین زمان میتواند تأثیر زیادی را در امنیت داشته باشد. اگر یک کارایی خاصی بسیار اهمیت دارد، شما باید این تصمیم را بگیرید که نباید اصلاً یک کامپیوتر را درگیر کنید. (منبع ۳)

به علاوه با دانستن اینکه استفاده رو به رشد از سیستم‌های دیجیتال باعث کاهش افزونگی می‌شود، مهم است که تأسیسات هسته ای این را درک کنند و اطمینان یابند که مقدار افزونگی کافی حفظ می شود. این ممکن است برای نمونه باعث شود که اطمینان یابیم وسایل پشتیبان دستی برای سیستم‌های حیاتی در هنگام یک خرابی وجود دارد.

ترویج اقتباس بیشتر از تکنولوژی های رمزگذاری و احراز هویت در نسل آینده ی ICS ها کلیدی است به دلیل اینکه سیستم‌های SCADA از نظر طراحی غیر ایمن هستند. افزودن احراز هویت در هنگام ارسال و دریافت ارتباطات و یا دستورها به این معناست که بخش‌های مختلف یک سیستم SCADA باید هویتشان را به همدیگر اثبات کنند -و اینکه ارتباطات یا دستورات که مخابره می‌شوند درست هستند. انجام این کار، حملات سایبری را که با فرستادن یک دستور غیر صحیح به یک ابزار که به صورت اتوماتیک آن را می پذیرد و یا ارتباطات را جعل می‌کند (برای مثال به همان صورت که توسط استاکس نت روی داد) خنثی می کند. و افزودن رمزگذاری به احراز هویت،‌محتوای ارتباطات و دستورات را توسط هکرها ناخوانا می‌کند و باعث می‌شود که حتی سطح بالاتری از امنیت به دست آید. منبع ۲۹ تاکید می‌کند: راه حل چالش ٬از نظر طراحی غیر ایمن٬ شامل رمزگذاری و احراز هویت است.

بادانستن اینکه انعطاف پذیری بی‌نظیر نسل کنونی از ICS همچنین باعث می‌شود که از نظر طراحی غیر ایمن باشند، ضروری است که انعطاف پذیریشان را محدود کرد. در حالی که طبیعت خاص محیط های صنعتی به این معناست که آن‌ها با چالش های امنیت سایبری مواجه می‌شوند که در محیط های IT خانه و دفتر وجود ندارند -مانند دشواری های وصله زنی- این خواص مخصوص همچنین به ما امکان اجرای راه‌های منحصر به فرد امنیت سایبری می‌دهند که در دومی ممکن نیست. برای نمونه ترویج ایجاد لسیت سفید، می‌تواند یک راه مهم برای تقویت امنیت سایبری در تأسیسات هسته ای باشد. به عنوان یک پروتکل ردوبدل اطلاعات که تنها به ترافیک و اعمالی اجازه ی اجرا شدن می‌دهد که در یک لیست مجوزدار به عنوان امن شناخته شده باشند، ایجاد لیست سفید در مقابل روش دفاع سایبری ایجاد لیست سیاه سنتی قرار می‌گیرد، مدلی که تحت آن تمام ترافیک و اعمال اگر در لیست بلوکه شده قرار نداشته باشند اجازه ی اجرا می یابند.

ایجاد لیست سفید می‌تواند در هر دو سطح ابزار و شبکه انجام شود. در سطح ابزار، روش شامل اجازه به وسیله برای انجام تنها مجموعه کمی از اعمال که برای نقش آن ضروری است می باشد. کامپیوتر تنها اجازه ی اجرای انواع خاصی از فایل‌های قابل اجرای از پیش تأیید شده را می‌دهد در مقابل روش کنونی که هر فایل قابل اجرای بر روی یک وسیله ی USB می‌تواند اجرا شود. این می‌تواند خطر آلودگی ایجاد شده در هنگام وارد کردن یک وسیله ی USB (که مسیر احتمالی استفاده شده توسط استاکس نت بود) را کاهش دهد.

ایجاد لیست سفید در سطح شبکه تنها شامل اجازه به ترافیک بین نقاط خاصی که برای فعالیت ضروری است می باشد. برای مثال به جای اجازه به یک کامپیوتر برای صحبت با تمام کامپیوترهای شبکه، لیست سفید به آن اجازه می‌دهد که تنها با تعداد محدودی از کامپیوترهای از پیش مشخص شده که نیاز به صحبت با آن‌ها دارد، حرف بزند.

محیط های صنعتی مخصوصاً مناسب لیست سفید هستند زیرا از نظر کارایی ثابت هستند و ما را قادر می‌سازد که دقیقاً مشخص کنیم کدام عمل یا ترافیک مجاز است. بیشتر محیط های IT دفتر و خانه دایما در حال تغییر هستند. در سطح ابزار، کاربران به صورت مرتب برنامه‌های جدیدی را در کامپیوترهایشان دانلود می‌کنند – چه برنامه‌های جدید یا آپدیت برنامه‌های موجود. در سطح شبکه، کامپیوترها به صورت مداوم به شبکه‌های والد اضافه و کم می شوند. این کامپیوترها همچنین در هنگام بازدید از وبسایتهای جدید و دریافت و ارسال ایمیلها به و از افراد جدید در تمام دنیا مقدار زیادی از ترافیک ناشناس را ایجاد می کنند. این باعث ایجاد سطح بالایی از عدم قطعیت می شود.

بر خلاف آن جهان صنعتی به نسبت ثابت است. در سطح ابزار، وصله زنی بسیار نادر است (بخصوص در محیط های هسته ای)، بنابراین تنظیمات ابزارها بسیار کم تغییر می‌کند. در سطح شبکه سیستمهای کنترل صنعتی بیشتر شامل کامپیوترهایی هستند که با کامپیوترهای دیگر صحبت می کنند؛ بنابراین ارتباطات و دستورات که اجزای مختلف آن سیستمها باید با سایر اجزای ردوبدل کنند باید الگوهای به نسبت ثابتی را دنبال کنند. این قابل پیشبینی بودن باعث می‌شود که قادر به تشخیص اینکه کدام اعمال و ارتباطات در محیط های صنعتی باید پذیرفته شود، باشیم.

درون یک محیط سیستم کنترل، مخصوصاً یک محیط هسته ای، توانایی اینکه این محیط ها را محافظت کنیم نسبت به یک محیط IT بسیار ساده‌تر است نه سخت تر.

ایجاد لیست سفید همچنین یک راه حل را برای چالش های وصله زنی تجربه شده در تأسیسات هسته ای ایجاد می کند؛ به این ترتیب که کارایی یک ابزار یا شبکه را محدود می‌کند و اهمیت وصله زنی سیستم‌ها کاهش می‌یابد و این در عوض باعث ساده شدن ایجاد لیست سفید می شود.

اگر شما زحمات مربوط به ایجاد لیست سفید را با زحمات مربوط به وصله زنی و مدیریت آسیب‌پذیری ها مقایسه کنید، حتی از نظر مقیاس هم به همدیگر نزدیک نیستند. (منبع ۹)

برای پیاده‌سازی لیست سفید اگر کنترل کننده های منطق قابل برنامه‌ریزی مدرن و خریداری شده در ۱۰ سال گذشته باشند، در صورت دیجیتالی بودن تنها یک ارتقای سفت افزار (firmware) یا یک کارت اترنت جدید مورد نیاز است. هزینه‌های مالی یک ارتقا قابل مدیریت است. در حقیقت بزرگترین بخش هزینه مربوط به آزمایش و برنامه‌ریزی های مورد نیاز انجام ایمن ارتقا است.

اگر یک سیستم قدیمی تر است، شاید ۲۰ یا ۳۰ سال دارد، در این صورت لیست سفید ممکن است ممکن نباشد. در این حالت سایر گزینه ها که می‌تواند امنیت را ایجاد کند مورد استفاده قرار می‌گیرد که شامل مدیریت فعال، پیاده‌سازی سیستم‌های محافظت در برابر نفوذ و سیستم‌های تشخیص نفوذ که ترافیک الکترونیکی را درون یک تأسیسات هسته ای برای تشخیص رفتار غیرطبیعی رصد می‌کنند، است. بعضی از این‌ها در ادامه بیشتر توضیح داده می شود.

سیستم‌های تشخیص نفوذ مانند رصد شبکه، که شامل آزمایش ترافیم درون یک تأسیسات هسته ای برای رفتار غیرعادی است می‌تواند تایسسات هسته ای را قادر کند تا روشی فعالانه تر را برای امنیت سایبری به کار گیرند. هنگامی که سیستم ترافیک غیرعادی را تشخیص می‌دهد که مطابق الگوی پذیرفته شده نیست، دارنده-اپراتور را خبر می کند.

برای بسیاری از تأسیسات (هسته ای و سایر)، اولین قدم در رصد شبکه کشیدن ترافیک مورد انتظار بین ابزارها برای ایجاد یک پایه ی استاندارد است. بسیاری از تأسیسات هسته ای هنوز این کار را انجام نداده‌اند و سایرین ممکن است این کار را در سطح جزییات کافی انجام نداده باشند.

بسیار ضروری است مه اپراتورها ابزارهایی را که دارند بشناسند، ارتباطشان با همدیگر را شناسایی کنند و سیستم‌های تکنیکی را قرار دهند که به محض اینکه هر کدام از آن‌ها تغییر کرد به اپراتور هشدار دهند. این کار خاص در برپایی صنعتی انجام نمی شود. این کار در درجه بالاتری انجام می‌شود که در صنعت هسته ای بسیار از حد کافی و همه جا حاضر فاصله دارد. (منبع ۹)

به دلیل اینکه مردم در مورد امنیت فکر نمی کنند، آن‌ها جریان های داده‌ای را در سطحی که برای امنیت مورد نیاز است ایجاد نمی کنند. روشی که در حال حاضر جریان های داده‌ای مستند می‌شوند به این صورت است که برای نمونه، این کامپیوتر داده را هر ۱۰ دقیقه به آن کامپیوتر می فرستد. اما چیزی که ما می‌خواهیم بدانیم، ارتباط میان آدرسهای IP یا پورتها و شکل داده است. برای نمونه اگر یک کامپیوتر سعی کند که یک آدرس IP خارج از شرکت من را در پورت ۸۰ مورد دسترسی قرار دهد، این یک پرچم قرمز خواهد بود زیرا نشانه ی این است که یک تروجان دسترسی در پشتی در حال فرستادن داده به یک سرور دستور و کنترل است. (منبع ۳)

کاربرد مجازی سازی -ساخت یک نسخه مجازی از یک ابزار، سیستم عامل یا شبکه- ممکن است یک فرایند مفید در کمک به درک جریان داده باشد و به عنوان یک راه مؤثر برای کشیدن این ارتباطات است. توسط مجازی سازی کل شبکه، می‌توانیم بدون درجه خطر موجود در هنگام آزمایش واقعی، در مورد جریانهای داده‌ای فرابگیریم.

ما می‌توانیم از محیط های مجازی برای یادگیری در مورد جریان های داده‌ای استفاده کنیم، بدون اینکه مجبور شویم به انجام آزمایش با شبکه خودمان و نگرانی از اینکه ممکن است چیزی را خراب کنیم. (منبع ۳)

علاوه بر این بررسی باید نه فقط در اطراف بلکه در کل شبکه سیستم کنترل صنعتی انجام شود. به دلیل اینکه پرسنل در تأسیسات هسته ای (و در حقیقت، به صورت عام‌تر در کل زیرساهت های حیاتی) معمولاً فقط بر روی دفاع پیرامونی تمرکز می‌کنند این کار باعث می‌شود بدافزارها بتوانند بدون شناسایی شدن در صورت عبور از دفاع پیرامونی به کار خویش بپردازند، آن‌ها باید درک کنند که باید تمام شبکه‌ها را مورد بررسی قرار دهند.

بیشتر افراد تمام تمرکز امنیتی خود را بر روی پیشگیری می‌گذارند و کار بسیار کمی را برای تشخیص و مهار انجام می دهند. این گرایش وجود دارد که بررسی شبکه بر روی سیستم پیرامونی باشد و گرایش بسیار کمی برای هر نوع از رصد شبکه درون سیستم کنترل وجود دارد. بنابراین مردم باید تمام شبکه هایشان را مورد نظارت قرار دهند نه فقط پیرامون را. (منبع ۲۷)

به علاوه ترویج به کارگیری دیودهای داده‌ای نوری ایمن در جایی که تاکنون مورد استفاده قرار نگرفته اند، می‌تواند به صورت چشمگیری امنیت سایبری را افزایش دهد. این کلیدی است زیرا تأسیسات هسته ای وجود دارند که تنها یک دیوار آتش برای محافظت شبکه سیستم کنترل صنعتی دارند.

درمورد چالش های زنجیره تامین، جهانی شدن صنایع به این معنی است که رفع کردن آسیب‌پذیری ها همچنان دشوار می ماند. هرچند بعضی کشورها قدم‌های مهمی را به طرف ملی سازی زنجیره تامینشان بر می‌دارند (در بخش هسته ای و فراتر از آن).

ژاپن بیشترین موفقیت را در اینجا در قادر کردن شرکتهای بومی برای ساخت کل بازه تولید برای نیروگاه های هسته ای اش داشته است. هرچند مطمینا میکروچیپ هایی با مبدأ ژاپنی مورد استفاده قرار می گیرد، منبع ۱۸ می‌گوید که نیروگاه های برق ژاپنی تقریباً ۱۰۰٪ ملی هستند؛ آن‌ها محصولاتی را می‌سازند که نیاز دارند.

بهترین گزینه برای کشورهایی که صنعت وسیع ملی مورد نیاز برای این کار را ندارند این است که آسیب‌پذیری زنجیره تأمین خود را به کمترین حد ممکن برسانند. برای نمونه روسیه، ملی سازی رنجیره تأمین خود را به عنوان یک اولویت می‌داند که شامل بخش هسته ای هم می شود. با دانستن دشواری های این کشور در تولید داخلی تمام محصولاتش، در کوتاه مدت روسیه به دنبال کاهش وابستگی اش به قطعاتی است که در کشورهایی تولید شده‌اند که آن‌ها را به عنوان کمتر دوستانه می‌شناسد؛ به و به جای آن قطعاتی را از چین که آن را به عنوان کشور دوستانه تر در حال حاضر می‌شناسد جایگزین می کند. روسیه این را به عنوان قدمی میانی در نظر می‌گیرد در حالی که همزمان ساخت صنعت ملی خود را ادامه می دهد. در بلند مدت روسیه امیدوار است که قادر به جایگزینی اکثریت قطعات با محصولات روسی شود.

در تمام سالهای گذشته یک بحث بزرگ در روسیه در مورد نیاز برای جایگزینی فوری قطعات و سخت افزارهای خارجی با نمونه‌های مشابه روسی وجود داشته است. این گرایش به تمام قلمرو ها و بخش‌های اقتصاد روسیه گسترش یافته است. (منبع ۱۲)

البته به دلایل مالی مهم است که تأسیسات هسته ای حیاتی ترین بخش بخشهای نیروگاه را از یک دیدگاه امنیت سایبری شناسایی کنند (قابل ذکر است، دارایی‌های سایبری حیاتی آنها) تا به آن‌ها بالاتری سطح از حاظت را اختصاص دهند. همان‌طور که منبع ۳ می گوید، این باید یک روش درجه‌بندی شده باشد؛ ما قادر یه انجام همه چیز برای همه ی سیستم‌ها نیستیم. بنابراین اولویت دهی خطرات سایبری کلیدی است.

۸. توسعه ی یک پاسخ سازمانی

خلاصه

این فصل یک سری از پیشنهادها را برای توسعه ی یک نظام پاسخ دهی در صنعت هسته ای غیرنظامی ارایه می دهد. این نظام با هدف کم کردن مشکلات امنیت سایبری که در بالا ذکر شد و همچنین پرداختن به سایر مشکلات ایجاد شده است. اساس آن بر روشهای سازمانی است که قابل مقیاس پذیر و انطعاف پذیرند و همچنین قادر به عمل با اطمینان و قدرتند، اما این با برجسته کردن نیاز به حفظ انرژی با منبع هسته ای انجام می‌شودتا اینکه از نیازهای تخصص امنیت که گاهی اوقات از نظر اقتصادی محدود کننده است استفاده شود.

نیاز برای سازماندهی

در امنیت سایبری، سازماندهی یک پیش نیاز برای همه چیز است. پاسخ‌های تکنولوژیکی بدون پشتوانه شکست‌خورده اند. بنابراین پاسخ‌های بر پایه داده داشته باشید. بدون سازماندهی، ارتباطات و کارهای مشارکتی شامل ذینفعان و افراد همواره ناکافی و غیرکارا خواهد بود. بدون سازماندهی، یک پاسخ استراتژيک سایبری کار نخواهد کرد.

باید به صورت منسجم عمل شود یعنی ذینفعان درگیر در نظام امنیت هسته ای آینده باید این را به عنوان هدفشان در نظر گیرند که اجزای یک فضای سایبری را که کلیدی برای به دست آوردن اهداف بخشی استراتژیک هستند، به یک اکوسیستم خودمختار تبدیل کنند نه اینکه به جای آن، همان‌طور که در حال حاضر انجام می شود، یک محیط مهار نشده تشکیل شده از اجزای متفاوت بسازند که هرکدام درگیر یک مبارزه ی تاکتیکی با مجموعه‌ای از خطرات است. ادراک ایجاد شده باید فراتر از امنیت سایبری به امنیت فیزیکی، امنیت پرسنل و ایمنی برسد. به علاوه مکالمات با‌معنا و مداوم بین ذینفعان IT و OT باید به عنوان یک ضرورت اساسی در نظر گرفته شود.

امنیت سایبری یک مفهوم چند بعدی است که نمی‌توان آنرا به سادگی درون سیاست گذاری های سنتی جای دهی کرد. در بخش هسته ای تمهیدات ایمنی و امنیت فیزیکی به تدریج توسعه پیدا کرده‌اند و در طول زمان کاملتر شده‌اند اما وابستگی سایبری که به سرعت در حال توسعه است ناهنجاری را در یک نظام امنیت ایجاد می کند. سه بخش اساسی (فیزیکی، مجازی و پرسنلی) در نرخ های متفاوتی تکامل می یابند، از لحاظ ظهور تهدید و توسعه قابلیت جبران کردن. این باعث یک پیچیدگی زیاد در مدیریت امنیت کلی می‌شود (با پیچیدگی بیشتر مشکلات خودنمایی تهدیدات درونی در تمام بخش‌های خطر).

این محیط باید در تمام زمان ها به ایجاد تعادل مناسب بین عمل‌های از پیش تنظیم شده و خود تعیین کننده ادامه دهد با این هدف که از هر گونه تمایل به طرف رکود کلی، که یک وضعیت جذاب برای گروه‌ها و افراد با هدف به چالش کشیدن سامان زنجیره تأمین انرژی هسته ای است، جلوگیری شود.

ارتباطات

استفاده های غیرقانونی مختلف از فضای سایبری به چالش در سطح سیستم بخش هسته ای غیرنظامی می افزاید. همان‌طور که تا کنون پیکربندی شده است، هرچند این بخش به عنوان یک اکوسیستم منسجم که امنیت سایبری در نظر گرفته شده باشد کنش و واکنش انجام نمی دهد. علی‌رغم تجربه پنجاه ساله ی توسعه ی یک فرهنگی مرتبط با ایمنی (و در حال حاضر بیشتر در ارتباط با امنیت) این اتفاق روی داده است. ذینفعان در حوزه ی امنیت هسته ای در سطح زیادی از هم مجزا هستند با وجود اینکه یک مجموعه ی کافی از مستندات سیاست امنیت ایجاد امنیت برای کامپیوتر دارند که به عنوان یک متصل کننده عملیاتی احتمالی کار می کند. در نتیجه آژانس های درون بخش ممکن است متوجه نشوند که توسط امنیت سایبری سایر ذینفعان تحت تأثیر قرار گرفته آن و یا عدم آن که بیشتر روی می‌دهد. این یک موضوع ارتباطی است که به صورت افقی بین تولیدکنندگان انرژی هسته ای وجود دارد اما همجنین به صورت عمودی در بین تمام زنجیره تأمین موجود است.

هماهنگی بهتر شده

در یک سطح ساده، اولویت ها برای یک نظام امنیت سایبری تنها به صورت سنتی هستند: بازدارندگی، جلوگیری، تشخیص و پاسخدهی. اما شکلی که این فعالیت‌ها هماهنگ می‌شوند حالت فرهنگ امنیت سایبری بخش هسته ای را مشخص می‌کند، که رابطه ی بسیار نزدیکی با ضرورت‌های مطلق فرهنگ ایمنی دارد که تاکنون در هسته ی صنعت بوده است.

تا اینجا چالش های در حوزه ی سایبری، در هر بخشی صنعتی که باشند معمولاً توسط یک مجموعه از پاسخ‌های تکنولوژيکی مدیریت شده اند. هرچند شواهد کافی موجود است و گویای این است که چالش اصلی که کل بخش را تحت تأثیر قرار می دهد،‌نیازمند یک مکانیزم پاسخ به همان اندازه وسیع است تا سطوح کلی بالاتری از امنیت را به دست بیاورد، در نتیجه اعتماد را در استفاده و نگهداری سیستم‌های اطلاعاتی و کنترل الکترونیکی ایجاد می کند. بدون منترل های مناسب رفتاری، پتانسیل های تکنولوژی برای ارایه ی کارایی های آینده در چرخه حیات انرژی هسته ای محدود می شود؛ شکل تهدید شروع به کشیده شدن می‌کند اما آگاهی به خودی خود به عنوان یک کاتالیزگر برای طراحی تکنولوژیکی سیستم‌های عملیاتی و دفاعی عمل نمی‌کند و باعث می‌شود که هماهنگ با جهان واقعی حرکت نکند.

برای تلاش در جهت اصلاح این عدم تعادل،‌سیاست های امنیت سایبری درون بخش باید جهت آمیختن دو روش گسترده‌تر شوند: نگرانی‌های واکنشی و از پایین به بالای در ارتباط با کامپیوتر و امنیت شبکه، همراه با امنیت شبکه و اطمینان بخشی؛ و روش از بالا به پایین کنترل شده توسط نیازهای مسئولیت های سطح بخش برای ارایه انرژی هسته ای با منبع هسته ای به صورت ایمن و با قیمت های اقتصادی. اگر این تبدیل سازمانی قابل به دست آوردن باشد، شکلدهی به سیاست‌های امنیت سایبری آینده برای هم جهت شدن با چشم انداز استراتژیک -بیشتر نیازهای کسب و کار هسته ای اما همچنین سیاست‌های جلورونده در مورد دولت و مقررات، به صرفه بودن از نظر هزینه و مخصوصاً جامع بودن – ممکن می شود.

عبارت امنیت سایبری و سایر عبارات مرتبط با آن به صورت گسترده ای مورد استفاده قرار می‌گیرند زیرا معنایشان مشخص و بدون کژتابی است اما تحقیق اصلی برای این گزارش ثابت می‌کند که هیچ ثباتی در روش برای مسایل سایبری در بخش بین‌المللی وجود ندارد و بخش هسته ای هم یک استثناء نیست. عدم وجود یک واژه نامه ی سایبری بین‌المللی هنوز هم مانع پاسخ‌های چندجانبه در تمام بخش‌ها به‌خصوص در هنگام به کار گیری در موانع زبانی می شود. حتی در بین افراد، تفسیر ٬سایبر٬ می‌تواند مجموعه‌ای از تناقضات و سؤالات پاسخ داده نشده را بپوشاند و یک چالش جدی را برای سیاست گذاران و کسانی که مسئول امنیت هستند ایجاد کند. برای مثال در چندین زیان تنها یک لغت برای ایمنی و امنیت وجود دارد.

حتی در بین افراد، تفسیر ٬سایبر٬ می‌تواند مجموعه‌ای از تناقضات و سؤالات پاسخ داده نشده را بپوشاند و یک چالش جدی را برای سیاست گذاران و کسانی که مسئول امنیت هستند ایجاد کند. برای مثال در چندین زیان تنها یک لغت برای ایمنی و امنیت وجود دارد

یک راه برای به دست آوردن هماهنگی در میان و اطراف گروه‌های ذینفع ممکن است این باشد که مجموعه از ذینفعان (مانند کادر تکنیکی) را در مرکز مسأله قرار دهیم و سپس پاسخ را در اطراف آن سازماندهی کنیم. هرچند تاسیس یک نظام یکپارچه و قوی در هر بخشی نیازمند یک ایده مشترک از امنیت سایبری -با تمرکز بر مسئاله و پاسخ به آن- است. در بالای درخت سیاست IAEA تعدادی توصیه درست در حال توسعه است اما در مرکز مشکل پایین دست یک عدم پایه مشترک در ساخت یک پاسخ احتمالی سایبری وجود دارد. این، توسعه یک روش مشترک برای مسایل سایبری را چالش برانگیزتر می کند. ساخت یک لغتنامه ی مشترک برای امنیت سایبری و در نتیجه یک نمایش تهدید مشترک به علاوه ی درنظر گرفتن تفاوت‌ها در فرهنگهای ملی از نظر مدیریت ریسک، بررسی امنیتی و پاسخهای عملیاتی همه مسایلی هستند که در ادامه و به صورت اورژآنسی باید در نظر گرفته شوند

مقررات

تهدیدی که بخش هسته ای در فضای سایبری با آن مواجه است به سرعت تغییر می کند، پیچیده و قوی است، در نتیجه یک مکانیزم پاسخ باید هم قدرتمند باشد و هم چابک. هرچند برخورد با نیازمندی های مقررات تنظیمی مسلماً منسوخ و بی مسئولیت که در یک محیط بسیار تنظیم شده (که هنجار فرهنگی در صنعت هسته ای است) اجرا می‌شود تنها مخرب است. چنان روشی به سرعت چابکی یک پاسخ احتمالی را که بر اساس فرهنگ بالغی است که بخش هسته ای در موارد ایمنی دارد، از بین می برد. به جای آن باید یک تعادل به خوبی قضاوت شده و بر اساس اطلاعات، در سیاست، مقررات و ارتباطات وجود داشته باشد. یک راه حل ممکن این است که مسئولین تنظیم کننده را با متخصصات امنیت سایبری آزموده شده که می‌توانند با سرعت و چابکی مناسبی عمل کنند، یاری داد.

تمهیدات مربوط به یک استراتژی که خطر ضربات سایبری را به جای واکنشی به فعال تبدیل می‌کند جهت بازداشتن دشمنان سایبری با افزایش درجه ی دشواری که آن‌ها در صورت حمله به بخش با آن روبه رو می شوند، مورد استفاده قرار می گیرد. این روش تهدیدات را به اهداف ساده‌تر منحرف می‌کند در حالی که همچنین اطمینان می‌یابد هر دشمن قطعی باید برای به نتیجه رسیدن سرمایه‌گذاری بیشتری بکند. یک نظام امنیتی سایبری هسته ای باید بخش را برای خرابکاران خطرناک کند در حالی که تعادل ظریفی را بین مقررات تجویز شده و قدرت دهی به افراد دارای دانش برای انجام کارهای مناسب در صورت ضرورت رعایت می کند. این روش باید در دید، دکترین و دانش بسیار پررنگ باشد و در کنترل متعادل باشد. توسعه ی فضای سایبر با ناامنی های درونی آن همواره بر هر نوع ساختار سلسله مراتب بین‌المللی سازی شده برای توسعه ی سیاست به جای پاسخ‌های عملیاتی پیشی می گیرد. این نوع نظام بیشترین آزادی را به آن‌هایی می‌دهد که نقشی را برای انجام در هنگام برخورد با خطرات امنیتی بخش دارند، در عین حال به یک روش وسیعتر برای امنیت سایبری از طریق یک سیاست شمولیت کمک می کند. همچنین به مقدار بیشتری بر ایجاد یک آگاهی مشترک از فضای سایبر، تهدیدهایش و روشهای عملیاتی اش و به علاوه، طیف قابلیت‌های امنیتی در دسترس شامل افزایش حفاظت برای به حداقل رساندن خطر، تکیه می کند.

پاسخ‌های تکنولوژیکی

چنان نظام امنیتی باید یک پاسخ تکنیکی را برای پرداختن به مسایلی که پیشتر توضیح داده شد (مانند وصله زنی و شکاف هوایی) را وارد کند. این می‌تواند درون یک روش سازمانی برای کاهش ریسک داخل شود و می‌تواند به صورت سریع و یک شکل برای افزایش سطح امنیت برای پرداختن به آسیب‌پذیری های حیاتی درون بخش به میدان عمل بیاید. بنابراین یک پاسخ کلی مناسب می‌تواند شامل یک اکوسیستم باشد که درون آن فعالیتهای آژآنس های مختلف پاسخ دهنده و افراد به جای اینکه با مهدیگر در تضاد باشند همدیگر را کامل می‌کنند و به صورت دوطرفه تقویت کننده همدیگرند: این می‌تواند شامل یک همکاری بسیار تنگاتنگ با کادر ایمنی و تیم امنیت فیزیکی در محل باشد. یک روش برای امنیت سایبری که افراد زیادی را از سراسر بخش و همچنین فراتر از آن (افراد تنظیم کننده ملی، برای مثال) در بر می‌گیرد، به ندرت خود را درگیر کنترل مرکزیت یافته می کند. عملیاتهای امنیت سایبری در تأسیسات هسته ای باید خودآگاه، خودمختار و خودبه خودی باشند و همچنین باید درون یک چارچوب مورد توافق که به احتمال زیاد توسط IAEA به صورت مرکزی تر هماهنگ شده است کار کند.

شواهد اندکی از حملات سایبری در بخش هسته ای غیرنظامی وجود دارد که احتمالاً به دلیل عدم افشای اطلاعات است (همان طور که در سایر بخش‌های حساس به اعتبار مانند بخش مالی این‌گونه است) اما همچنین دلیل دیگر آن عدم اکتشاف است. پاسخ‌های کنونی به سوء‌استفاده از فضای سایبری توسط خرابکاران از نظر خصوصیتی فاقد چابکی و کارایی است. تهدیدهای سازماندهی شده نیازمند پاسخ‌های سازماندهی شده از کل بخش هستند که ضرورتاً شامل مدیریت در بالاترین سطح (پشتیبانی شده توسط مشاوران دارای اطلاعات به روز) با ورودی های قدرتمند و آگاهانه از ذینفعان مختلف ورودی و خروجی است. قابلیت‌های تکنولوژیکی درگیر در محافظت، تشخیص و پاسخ دهی نیازمند این موارد است: تبعیت از خطریاب ها و تشخیص هدایت و توصیه‌های مخصوص امنیت سایبری که IAEA به نمایندگی از کشورهای عضوش در حال توسعه است.

حاکمیت

حاکمیت امنیت سایبری در این بخش باید قادر به ترویج بحث‌هایی پیرامون دو عامل باشد. اول، پاسخ‌ها باید به گونه‌ای مدیریت شوند که هنجاری ایجاد کنند که استفاده از تکنولوژی های ارتباطی و اطلاعاتی (ICT) را پشتیبانی می‌کند برای اطمینان از تولید ایمن و کارای انرژی هسته ای در حالی که دشواری هارا برای عامل تهدید افزایش می دهد.

دوم، مدیران امنیت سایبری باید یک بعد اشتراکی داشته باشند که شامل تمام ذینفعان کلیدی و سازمان هاست. واضح است جایی که آسیب‌پذیری ها در محافظت از زیرساخت و اطمینان از اطلاعات باقی می مانند، احتمال یافته شدنشان وجود دارد (چه تصادفی یا بر اساس نقشه) و توسط فرد خرابکار مورد سوءاستفاده قرار می گیرند. یک روش اشتراکی می‌تواند امنیت سایبری را قادر به تبدیل شدن به یک فرایند پویاُ و خودآموخته بر اساس اصول عملیاتی مشترک برای مقابله با تعدیدهای در حال تکامل، می‌کند و از یک چرخه دکترین بر اساس ٬چرخه بوید٬ (Boyd cycle) بهسازی فرایند مستمر (رصد، جهتدهی، تصمیم و غیره) سود می‌برد. اگر به هر ذینفع فرصت آموختن از تجربه دیگران داده می شد، سطح کلی امنیت سایبری در میان یک بخش انتخاب شده افزایش می یافت (و نشان داده شده است که در خدمات مالی بریتانیا از طریق مفاهیمی مانند نیروی کار مجازی(Home office 2010) چنین کرده است).

به این ترتیب پاسخ‌های مؤثر و پایا در فضای سایبری نیازمند یک آگاهی مشترک، یک اشتیاق برای مشارکت و توسعه ی یک غریزه برای خطرپذیری است که ممکن است به عنوان یک فرهنگ امنیت سایبری هم توضیح داده شود. اما دستیابی به این،‌یک بار دیگر وابسته به توسعه ی یک مدیریت واقعاً آگاه در بالای اکوسیستم و پس از آن زیردستانش است.

مدیریت ریسک

رسیدن به امنیت مطلق در فضای سایبری نیازمند این است که تمام تهدیدها، مجموعه ابزارهایشان و مسیرهای حمله شان شناسایی و جدا شوند و تراکنش های خاصی قبل از آنکه به یک خطر بحرانی تبدیل شوند، مورد ممنوعیت قرار گیرند.

هرچند با در نظر گرفتن پیچیدگی اینترنت،‌ سرعتی که بدافزارهای توسعه می یابند و غیرقابل پیشبینی بودن اجزای انسانی محیط،‌چنان ایمنی کاملی یک تخیل است و حتی یک تخیل مطلوب هم نیست، با وجود محدودیت‌هایی که بر فرایندهای صنعتی اعمال می‌شود.

بنابراین نیازهای یک نظام امنیت سایبری هسته ای باید مدیریت و به حداقل رسانده شود به جای آنکه تهدیدها از فضای سایبری برداشته شوند، و همچنین ارتباط این تهدید ها با آسیب‌پذیری ها،‌شباهت یک حمله و تأثیرات احتمالی در صورت موفقیت یک حمله باید ارزیابی شوند. بنابراین امنیت سایبری تبدیل می‌شود به یک مسأله مدیریت خطر درون محیطی که عنصر کلیدی موجودیت پاسخگو توسعه ی سرعت و چابکی است.

شمولیت

یک روش تکنولوژیکی تنها برای حل پیچیدگی فضای امنیتی کافی نخواهد بود. یک روش برای امنیت سایبری که به صورت کامل و یا عمده تکنولوژیکی است، فاقد عمق است و به مدافع توانایی توسعه ی یک سری به هم مرتبط از لایه‌های امنیت را که هرکدام برای حمله کننده یک مانع ایجاد می‌کنند،‌ نمی دهد. درک برخورد بین جنبه‌های تکنیکی، انسانی، سازمانی و مقرراتی به درون قلب حل و یا حتی به حداقل رساندن مشکل امنیت سایبری در هر بخشی می‌رود چه رسد به میدان از نظر سیاسی حساس تولید انرژی هسته ای.

با دانستن پیشرفتگی تکنولوژیکی واسط سایبری، سرعت تغییر و شیوه ای که کاربر از کاتالیزگر اینترنت درجات بالایی از نوآوری را می‌خواهد، امنیت درون زیرساخت ICT می‌تواند به عنوان یک مشکل امنیت بسیار بزرگ‌تر از توانایی‌های تحلیلگران، صنعت کاران و سیاست گذاران دیده شود. این وضعیت به صورت ملی و بین‌المللی و درون خود بخشهای صنعتی وجود دارد و در آن مجموعه پیچیده‌ای از مسئولان تنظیم کننده برای قرار دادن علایم خودشان در ساختار امنیت سایبری حوزه خود تلاش می کنند. اما این وضعیت الزاماً در بخش هسته ای، جایی که ذینفعان کمتری هستند، نباید وجود داشته باشد، آن‌ها معمولاً با همدیگر آشنا هستند و فرهنگ ٬اشتراکی٬ به وضوح بیشتری پذیرفته شده است (به خصوص از دید لنز سنتی ٬ایمنی٬). این اصل پایه در ارایه ی ایمنی هسته ای، با وجود یاری دهی مناسب توسط تنظیم کنندگان و توسعه دهندگان یک مدل قابل اعمال از پاسخ‌های مورد نیاز، پتانسیل تبدیل به یک امنیت سایبری توسعه یافته در این بخش را دارد.

تنظیم پاسخ‌های آینده

در این مفهوم دشوار از امنیت سایبری، بعضی قابلیت‌ها می‌تواند به عنوان عقل سلیم در نظر گرفته شود که همراستا است با اصول کلی در سیستم‌های مدیریت خطر که بیشتر منابع در بحرانی ترین آسیب‌پذیری ها مصرف شده اند. هرچند فلسفه ی انجام اعمال فعالانه برای به حداقل رساندند خطر هنگامی که شناسایی شده‌اند،‌ به جای تمرکز بر پاسخ‌ها در هنگام وقوع -که معمولاً به آن مدیریت خطر ٬شیفت دهی به چپ٬ گفت می شود(Jonas 2011)- هم به فعالیت‌های بازدارنده و کمتر وابسته به منبع (و ارزانتر) تعلیم، آموزش و تمرین اشاره می کند.

ویژگی کلیدی پاسخ، چابکی و ابتکار عمل است و از هردو روش ناوابسته به عامل و بر اساس خطر استفاه می کند.

چابکی و ابتکار عمل. همان‌طور که پیشتر گفته شد، بازه ی تهدیدات سایبری چنان وسیع است و طیف ایجاد کنندگان تهدید چنان گسترده است که یک فلسفه ی دفاع سایبری ٬خطی در ماسه٬ به معنی دو چیز است. اول، دشمن سایبری چابک و باهوش (و دارای منابع) که به دلیل فرایندهای کسب وکاری طولانی کارش آسان شده است و دارای ابتکار عمل خوبی در مبارزه است و مجبور نیست که برای به دست آوردن و حفظ ابتکار عمل به سختی کوشش کند. دوم (همان طو که از مصاحبه‌های برای این پروژه ثابت شد) پاسخ به تهدیدهای سایبری بیشتر تمایل دارد که واکنشی باشد تا پیشبینانه، به گونه‌ای که واکنش‌های تنها زمانی روی می‌دهند که یک تهدید دیوارآتش را مورد حمله قرار می‌دهد و یا درون آن کشف می‌شود (اگر در کل کشف شود). به بیان دیگر نقطه‌ای که مکانیزم پاسخ این بخش شروع به پرداختن به تهدیدهای سایبری می‌کند، هنگامی است که آن تهدیدات کاملاً توسعه یافته‌اند و در قدرتمندترین وضعیتشان هستند. قبل از اینکه این اتفاق بیافتد، ممکن است حملات در بخش‌های دیگر تکرار شده باشد، به صورت ملی یا بین المللی، به‌خصوص آن‌هایی که شامل یک برتری بر سیستم‌های کنترل صنعتی هستند. پاسخ‌های امنیت سایبری بخش هسته ای باید به چابکی هرچه تمام تر مورد جستجو قرار گیرند و باید بر از بین بردن تعادل دشمن با به دست آوردن و حفظ ابتکار عمل تمرکز شود و باید اعمال ممکن بر اساس اطلاعات باشند. بخش اطلاعاتی که شامل اسکن افقی، تحقیق و توسعه(R&D) و اطلاعات از سایر عامل های دیگر در بخش، است به این ترتیب در تعیین ماشه ای که مکانیزم پاسخ را به راه می‌اندازد یاری رسان است.

یک روش نا وابسته به عامل

یک روش ٬ناوابسته به عامل٬ که در آن قابلیت بدون توجه به عامل تهدیدات خاص (و شناخته شده) توسعه می یابد، مورد نیاز است به این دلیل که عوامل تهدید بسیار متنوع هستند و می‌توانند بسیار سریع تغییر کنند. نکته مهم دانش این است که یک دشمن (هر دشمنی) چه کاری می‌تواند انجام دهد و داشتن سیاستها، فرایندها و تجهیزات لازم برای رفع (و یا پیشبینی) آن چالش، از هرجا که ریشه گرفته است و هرزمان که روی می دهد.

یک روش برمبنای خطر

منطقی نیست که انتظار داشته باشیم که تمام تهدیدهای سایبری را برای همیشه از بین ببریم و همچنین ممکن نیست که تمام استفاده های (واقعی یا احتمالی) مجرمانه و متخاصمانه از زیرساخت ICT جهانی را فیلتر کرد. هرچند یک روش براساس خطر برای امنیت سایبری باید:

- نشان دهد استفاده قانونی از ICT نباید فارغ از نتایج مضر ممکن در نظر گرفته شود.

- ما را قادر کند که امنیت سایبری را بر اساس تناسب ارزیابی کنیم: منافع گرفته شده می‌تواند در برابر مجازات های ممکن قرار گیرد و به این ترتیب منافع می‌تواند اولویت دار شود.

- چابکی و انعطاف پذیری را افزایش دهد: در عین اینکه چالش های امنیت سایبری تکامل می یابند، اولویت ها می‌تواند دوباره تنظیم شود.

- اجازه ی تنظیم سیاست‌های امنیت سایبری را ب صورت کلی و یا در سطح سیستم بدهد به گونه‌ای که خطرات و تهدیدهای یک بخش قابل پوشاندن توسط منافع و برتری‌های بخش دیگری باشد.

یک نظام امنیت سایبری

در تبدیل مدیریت امنیت سایبری در مسیر پیشنهاد شده در گزارش حاضر، منطقی و مفید است که این تلاش‌ها را تحت جنبه‌های یک نظام امنیت سایبری در سطح بخش تعریف کنیم. چنان نظامی یک متدولوژی را برای سازماندهی تلاشها از مسیر توسعه ی ملی و بین‌المللی سیاست‌های تواناساز تعریف می‌کند در عین حال تصدیق می‌کند که عملیات های موفق امنیت سایبری باید توسط اولیای مالی به نیروگاه های هسته ای موکل شوند.

یک نظام موفق و پایا نظامی است که به صورت هوشمندانه و پاسخ دهنده درون محوطه مربوطه کار می کند، کاملاً با شکل خطر، تهدیدهای همراهش و مجموعه ی اقدام‌های متقابل به روز می ماند،

هر سیستم مدیریت که به صورت از مرکز کنترل شده یا بیش تجویز باقی می‌ماند باعث کاهش سرعت و چابکی در پاسخدهی می‌شود و باعث یک شکاف وسیع شونده میان تهدیدها و پاسخ‌ها می‌شود در نتیجه خطر را افزایش می دهد. یک نظام موفق و پایا نظامی است که به صورت هوشمندانه و پاسخ دهنده درون محوطه مربوطه کار می کند، کاملاً با شکل خطر، تهدیدهای همراهش و مجموعه ی اقدام‌های متقابل به روز می ماند، روش رژيم مناسب‌ترین پایه را برای یک استراتژی امنیت سایبری بخشی تأمین می‌کند زیرا می‌تواند مجموعه ی زیادی از عاملها، آژانسها و ذینفعان را شامل شود و به آن‌ها مسئولیت دهد (نه به صورت مستقیم زیرا انجام آن ایجاد مقاومت می‌کند و بر تأخیر می افزاید). این سیستم می‌تواند به اندازه کافی چابک باشد (در عین حال بدون از دست دادن تمرکز) برای رفع یک چالش امنیتی به سرعت در حال تکامل و تبدیل.

یک استراتژی فعال برای امنیت سایبری به این ترتیب می‌تواند در یک سری از مراحل توسعه یابد:

- با تاسیس یک سازمان چابک

- با ایجاد یک سیاست بخشی

- با برنامه‌ریزی دقیق و از بین بردن تعارضات

- از طریق توسعه ی پاسخ دهی

بر اساس تحلیل بالا، یک نظام مدیریتی امنیت سایبری بخشی مؤثر باید:

- یک روش در سطح بخش را از بالاترین سطوح تا تک تک افراد ترویج دهد

- یک محیط جلو رونده را پشتیبانی کند که برای حفظ سرعت طراحی شده است و ایجاد تعادل مناسب بین مقررات و نیاز برای پرورش یک فرهنگ از مسئولیت های سازمان و افراد را انجام دهد.

- ورودی از تمام منابع دردسترس متخصص سایبری بگیرد

- یک محیط رسمی و به خوبی تأمین مالی شده برای ترویج و پرورش امنیت سایبری درون بخش ایجاد کند

- جریان آزاد اطلاعات را بین تمام ذینفعان ایجاد کند و یک گروه آگاه ایجاد کند که در آن اصول کلیدی رهبری، مسئولیت و حسابداری بتواند به وضوح تشخیص داده شود.

- مکانیزم لازم برای ایجاد آمادگی عمیق برای چالش های امنیت سایبری را ایجاد کند، این‌ها قادر به ایجاد یک پاسخ هماهنگ و چابک شامل بررسی افق و R&D برای توسعه ی مرزهای نظام تا بیشترین حد ممکن هستند.

- کانالهای ارتباطی غیرمبهم برای آژانس های تخصصی ملی و بین‌المللی تعریف کند

در حالی که جامعه در کل بیشتر درگیر مشکل امنیت سایبری می‌شود، پیشرفت در بخش هسته ای سخت تر شده است. هرچند که IAEA تعدادی راهنمای درست برای امنیت کامپیوتری توسعه داده است، تا کنون فرهنگ این بخش بیشتر بر ایمنی تمرکز کرده است. این باعث شده است که پیاده‌سازی امنیت سایبری بیشتر به صورت غیرفعالانه، دفاعی و غیر هماهنگ باشد؛ هردو مورد چابکی و سازماندهی در این بخش به مقدار کمی موجود است. این باعث ناهماهنگی هایی در پیاده‌سازی تکنیکی شده است.

راه سازماندهی شده‌ای که تهدیدات از طریق اینترنت نمایش داده می‌شوند نیازمند یک پاسخ سازمانی توسط بخش هسته ای غیرنظامی است که ضرورتاً شامل رهبری مطلع در بالاترین سطح، همراه با کمک‌های پویا توسط مدیران زیردست و کارمندان و تمام گروه ذینفعان شامل اعضای جوامع وسیعتر امنیت و ایمنی. ورودی های عالمانه و قدرتمند از جوامع درونی و افراد و همچنین آزانس های خارجی مانند اعضای دولت مورد استقبال نظام امنیت سایبری قرار می گیردند. هر یک از این ذینفعان یک نقش برای انجام دادن در سیستمی دارند که باید سرعت بالایی ایجاد کند و یک محیط بسازد که در آن نوآوری برای رشد پذیرفته شده است و فرایندهای ناکامل به چالش کشیده می شوند.

۹. نتیجه‌گیری

این گزارش دامنه ی چالش های امنیت سایبری را در تأسیسات هسته ای مورد آزمایش قرار داد و تعدادی از راه حل‌های مخصوص را برای چاش های شناسایی شده به علاوه ی چندین توصیه ی عملی برای صنعت هسته ای در یک مقیاس وسیعتر ارایه داده است.(بر ای راحتی بیشتر این‌ها در پایان خلاصه ی عملی لیست شده اند.)

شاید بزرگترین مشکل امنیت سایبری که صنعت هسته ای با آن روبه رو است این باشد که بسیاری از افراد در این بخش به صورت کلی خطر را درک نکرده اند، بنابراین مرحله کلیدی اول این است که دستورالعملهایی برای ارزیابی و اندازه‌گیری هرچه دقیقتر این خطرات طراحی توسعه داده شود. این به مدیران عامل و هیات مدیره ی شرت کمک می‌کند که چه چیزی مورد خطر است و همچنین به آن‌ها با یک منطق اقتصادی روشن کمک می‌کند تا در امنیت سایبری سرمایه‌گذاری کنند. توسعه ی بیمه ی سایبری با ارتباطات قدرتمندش با معیارهای خطر ممکن است یک ابزار مهم برای ترویج و توسعه ی دستورالعمل های خطرپذیری سایبری باشد. در برخورد با چالش های مربوط به عامل انسانی، همچنین مهم است که آگاهی را میان هردوگروه مهندسان و افراد مورد قرارداد در مورد خطر های موجود در ایجاد ارتباطات غیرمجاز یا وصل کردن ابزارهای USB شخصی به تأسیسات شرکت افزایش داد. تمهیداتی که افشا و به اشتراک گذاری اطلاعات را ترویج می‌دهند هم می‌توانند یک نقش مهم را در افزایش امنیت سایبری ایفا کنند، به همین صورت استانداردهای تنظیمی و سایر تمهیدات سیاستی، ارتباطات بهتر برای پرکردن شکاف های فرهنگی و پیاده‌سازی راه حل‌های تکنیکی هم یاری دهنده هستند.

صنعت هسته ای به عنوان یک کل، نیازمند است به توسعه ی یک تلاش قوی برای گرفتن ابتکار عمل در فضای سایبری و همچنین تأمین مالی ارتقا و پرورش یک فرهنگ از امنیت سایبری، تعیین اولویت های سرمایه گذاری، و اطمینان از اینکه تأمین مالی های کافی و مداوم به ایجاد یک استراتژی مدیریت خطر امنیت سایبری بین‌المللی انجام شده، و تشویق جریان آزاد اطلاعات بین تمام ذینفعان. این، صنعت را مجبور می‌کند تا مکانیزم و برنامه‌های هماهنگی عملی را برای برخورد با کمبودهای تکنیکی شناسایی شده و همچنین یافتن تعادل درست بین مقررات و مسئولیت های فردی توسعه دهد.

گزارش حاضر همچنین تعدادی حوزه های مهم را برای کارهای آینده مشخص می کند. با دانستن اینکه کشورهای در حال توسعه بیشتر در برابر این خطرات آسیب‌پذیر تشخیص داده شده اند، نیازهای مخصوص آن‌ها باید ارزیابی شود تا منابع به صورت کاراتری برای مبارزه با خطرات مخصوص شناسایی شده مصرف شود. عدم آمادگی مشخص برای یک حالت اضطراری مقیاس وسیع امنیت سایبری ، به‌خصوص آن‌هایی که در خارج ساعات کاری عادی روی می‌دهند همچنین گویای این است که مطالعات و تمرینات برنامه‌ریزی بر اساس سناریو باعث درک بهتری می‌شوند از اینکه چگونه یک وضعیت می‌تواند در یک بحران آشکار شود و همچنین در توسعه ی برنامه‌های پاسخ در تمام صنعت به با کمک می کند.

تعدادی از یافته ها در این گزارش ممکن است یک ارتباط وسیعتری فراتر از بخش هسته ای داشت هباشند زیرا بسیاری از چالش های توضیح داده شده در اینجا به صورت عام در تمام زیرساخت های حیاتی مشترکند. مثالهایی از راه حل‌هایی که می‌تواند در تمام بخش‌ها به کار گرفته شود،تلاش هایی برای پر کردن شکاف ارتباطی، اقتباس تکنیک لیست سفید و ساخت CERT های صنعتی است.

هدف اصلی این تلاش تحقیقاتی برای گسترش ایده‌های عملی و ارزشمند برای تصمیم گیران علی زغم افزایش ایمنی و امنیت در صنعت هسته ای است. ما امیدواریم که یافته ها و نتایج بحث‌های مهیجی را در بخش هسته ای در مورد خطرات -و پاسخ‌های به- یک بازه ی وسیع از حملات ممکن سایبری ایجاد کند و در نتیجه به صورت کلی به صنعت و جوامعی که به آن‌ها سرویس می‌دهد نفع برساند.