مجله علمی- پژوهشی "پدافند الکترونیکی و سایبری"

سال اول، شماره ۴، زمستان ۱۳۹۲، ص ۶۶-۵۵

مدل‌سازی تیم واکنش سریع به حملات رایانه‌ای استانی

علی ناصری[۱]، سمیه حجازی[۲*]

۱- استادیار دانشگاه جامع امام حسین (ع)، ۲- کارشناس ارشد مهندسی فناوری اطلاعات، دانشگاه شیراز

(دریافت: ۹۲/۷/۲۷ ، پذیرش: ۹۲/۱۱/۱۴)

چکیده

تیم واکنش سریع به حملات رایانه‌ای نقش به‌سزایی در امن‌سازی فضای سایبر دارد. با توجه به استقلال شرکت مخابرات استان‌ها در ارائه سرویس‌های شبکه، لازم است با لحاظ نمودن همه جوانب نسبت به راه‌اندازی این تیم اهتمام ورزید. در این مقاله با مطالعه مفاهیم پاسخ‌گویی به حوادث امنیت رایانه‌ای و مراحل پیشنهادی CERT/CC برای توسعه تیم‌های پاسخ‌گویی به حوادث امنیت رایانه‌ای، به مدل‌سازی این تیم برای شرکت مخابرات استان‌ها که هدف آن ارائه خدمات پاسخ‌گویانه، پیشگیرانه و مدیریت کیفیت در حوزه امنیت شبکه در داخل و خارج شرکت است، پرداخته‌ایم. در این مدل‌سازی تحلیل وضع موجود و نیازمندی‌های فضای تبادل اطلاعات شرکت مخابرات استان، مبنای تصمیم‌گیری در خصوص ساختار و طرح پیاده‌سازی TCL-CERT بوده و این طرح مبنای توسعه خط مشی‌ها، رویه‌ها، طرح‌ها، نقش‌ها، مسئولیت‌ها، فرایندها و تعاملات آن با CERTهای ملی است.

واژه‌های کلیدی: حوادث امنیتی رایانه‌ای، CERT، حادثه، خدمات پیش‌گیرانه، خدمات واکنشی، مدیریت حادثه، خدمات پاسخ‌گویانه

۱. مقدمه

تیم واکنش سریع به حملات رایانه‌ای[۱] (CSIRT) وظیفه مهار حوادث رایانه‌ای و انجام اقدامات لازم برای رفع حوادث و همچنین جلوگیری از حوادث را به عهده دارد. به سازمان یا تیمی که سرویس‌ها و حمایت‌هایی در جهت جلوگیری، رسیدگی و پاسخ‌گویی به حوادث امنیتی رایانه‌ای برای محدوده عملکرد آن فراهم می‌نمایند، تیم پاسخ‌گویی به حوادث رایانه‌ای گفته می شود [۵]. اولین گروه پاسخ‌گویی به حوادث رایانه‌ای، در سال ۱۹۸۸، بعد از اینکه کرم موریس ده درصد رایانه‌هایی را که به اینترنت متصل بودند آلوده کرد، در دانشگاه کارنجی ملون[۲] به‌وجود آمد [۱و۲]. حملات از کاراندازی سرویس، انتشار بدافزارها، دسترسی غیرمجاز، استفاده نامناسب و حملات ترکیبی، منجر به حوادث امنیتی رایانه‌ای می‌شوند[۴]. برخی از مهم‌ترین نکات جهت امنیت برنامه های کاربردی، سامانه‌ها و شبکه‌ها، شامل مدیریت وصله ها، امنیت میزبان‌ها، ممانعت از انتشار بدافزارها، امنیت شبکه، آموزش و اطلاع‌رسانی به کاربران می‌باشد[۴].

سرویس‌های ارائه شده توسط تیم پاسخگویی به حوادث امنیتی رایانه‌ای در سه دسته: سرویس‌های پاسخ‌گویانه، سرویس‌های پیش‌گیرانه و سرویس‌های مدیریت کیفیت امنیتی دسته‌بندی می‌گردند [۶]. عناصر ایجاد یک تیم پاسخگویی به حوادث امنیتی رایانه‌ای کارا، چارچوب عملیاتی، چارچوب سیاست‌گذاری و سرویس، اطمینان کیفیت، انعطاف‌پذیری و سازگاری هستند[۳]. در ادامه CSIRC[۳] و انواع آن شرح داده می‌شود. در بخش سوم مدیریت حوادث امنیتی رایانه‌ای، در بخش چهارم اقدامات ایجاد CSIRT و در بخش پنجم مدل‌سازی CSIRT شرکت مخابرات استان ارائه می‌گردد. در نهایت در بخش شش نتیجه گیری ارائه شده است.

۲. CSIRC و انواع آن

قابلیت پاسخ‌گویی سریع و موثر به حملات رایانه‌ای، یک عنصر اساسی در ایجاد یک محیط امن برای شبکه‌ها است و برای تشخیص سریع، کاهش زیان، خرابی و ضعف‌های موجود و نیز بازیابی سرویس‌های رایانه‌ای ضروری است.

1- Computer Security Incident Response Team (CSIRT)

* رایانامه نویسنده پاسخگو: somayehejazi@gmail.com

2- Carnegie Mellon

3- Computer Security Incident Response Capability

در عین حال، این قابلیت به طراحی و منابع قابل توجهی نیاز دارد[۴]. در ادامه، برخی از مزایای CSIRT بیان می‌گردد:

- پاسخ به حوادث به‌صورت روشمند با طی مراحل مناسب.
- بررسی و ارزیابی امنیت زیرساختار، شامل بررسی سخت افزار و پیکربندی نرم‌افزار، مسیریاب‌ها، دیوارهای آتش و سرورها، پویش-گرهای ویروس و تست‌های نفوذ.
- کمک به پرسنل در جهت پوشش هر چه مؤثرتر و سریع‌تر حوادث امنیتی.
- کاهش از دست روی و یا دزدی اطلاعات و یا قطع سرویس‌ها.
- استفاده از اطلاعات به‌دست آمده در خلال بررسی حادثه، برای آمادگی بهتر بررسی حوادث آینده و حفاظت قوی‌تر از سامانه‌ها و داده‌ها.
- توسعه رویه‌های عملیاتی استاندارد[1] (SOP) برای رعایت اولویت‌های سازمان و پاسخ‌های سریع‌تر و مؤثرتر.
- برخورد صحیح با موضوعات حقوقی پیش آمده در خلال حوادث [۴].

ساختارهای مختلفی برای تیم‌های CSIRT وجود دارد که وظایف و حتی نام‌های مختلفی دارند. تفاوت‌های CSIRTها، در ماموریت‌ها (مقاصد فراگیر و تغییرناپذیر) و اهداف (مقاصد کاربردی تر و تغییرپذیر) آنها می‌باشد. همچنین، محدوده عملکرد CSIRT و سرویس‌های ارائه شده، تعاریف و مجموعه اصطلاحات سازمان در آن نقش دارد. تیم‌ها در بخش‌های مختلف تجاری، دولتی، اجرای قانون، نظامی، آموزش و تحقیقات، فرا ساختارهای بحرانی، ارتباطات و فناوری اطلاعات و... ممکن است تشکیل شوند. در ضمن، همه تیم‌ها اختیارات، نقش در فرآیندهای مدیریتی، سرویس‌ها، مدل سازمانی، راهبردهای تامین بودجه و مدل‌های درآمدزایی، شیوه گزارش‌دهی یکسانی ندارند[۳]. هر CSIRT مطابق با ماموریت خود، سرویس‌های متفاوتی می‌تواند ارائه کند. هر تیمی باید سرویس‌های خود را بر اساس نیازهای سازمان تعیین کند[۵]. در جدول ۱ سه دسته‌بندی اصلی برای سرویس‌های CSIRT ارائه شده است. CSIRTها از لحاظ شکل، اندازه و حوزه عملکرد، به CSIRTهای داخلی، ملی، مراکز هماهنگی، مراکز تحلیل، تیم تولیدکنندگان و ارائه‌دهندگان سرویس پاسخ‌گویی به حوادث تقسیم می‌شوند [۷].

CSIRTهای پراکنده، گام‌های پاسخ به حوادث واقعی امنیتی و راهبردهای تخفیف اثر را انجام می‌دهند.[2] CERT هماهنگ‌کننده، همزمان‌سازی آمار و گزارش‌های حوادث همه حوزه‌ها را جهت تعیین جایگاه امنیتی سازمان و آسیب‌پذیری‌های آن، انجام می‌دهد[۳].

CSIRTهای هماهنگ‌کننده ملی، با کمک به محافظت از سامانه‌ها، کشف، تشخیص و تحلیل آسیب‌های امنیتی، حفاظت در مقابل فعالیت‌های مخرب، وقوع حوادث امنیتی سایبر، هماهنگی و پاسخ موثر و سریع به حملات رایانه‌ای، ترویج و کمک به سازمان‌های محدوده عملکرد، برای توسعه قابلیت‌های مدیریت حادثه، می توانند نقش مهمی در این راستا ایفا کنند[۱۲].

جدول ۱. سرویس‌های CSIRT [۶]

سرویس‌های پاسخگویانه	سرویس‌های پیشگیرانه	سرویس‌های مدیریت کیفیت امنیت
هشدارها و اخطارات	اعلان خبر	تحلیل ریسک
رسیدگی حادثه تحلیل حادثه پاسخ به حادثه پشتیبانی پاسخ به حادثه هماهنگی پاسخ به حادثه	نظارت بر فناوری	طرح ریزی ترمیم حادثه و دوام فعالیت‌های تجاری
	تشخیص یا بازرسی امنیتی	رایزنی امنیتی
	پیکربندی و نگهداری از ابزارهای امنیتی، برنامه‌های کاربردی و فراساختارها	آگاهی‌سازی و هوشیارسازی
رسیدگی آسیب‌پذیری تحلیل آسیب‌پذیری پاسخ به آسیب‌پذیری هماهنگی پاسخ به آسیب‌پذیری	توسعه ابزارهای امنیتی	تعلیم و آموزش
	سرویس‌های تشخیص مزاحمت	ارزیابی محصول یا گواهینامه
	انتشار اطلاعات مرتبط با امنیت	
رسیدگی به کدهای آسیب‌رسان تحلیل کدهای آسیب‌رسان پاسخ به کدهای آسیب‌رسان هماهنگی پاسخ به کدهای آسیب‌رسان		

1- Standard Operating Procedure (SOP)

2- Standard Operating Procedure (SOP)

CSIRTها دارای مدل‌های سازمانی مختلفی از قبیل تیم‌های امنیتی موجود، مدل متمرکز، مدل توزیع شده، مدل ترکیبی و مدل هماهنگ‌کننده می‌باشند. در سازمان‌های کوچک، استفاده از مدل متمرکز، مناسب‌تر است؛ حال آنکه مدل ترکیبی برای سازمان‌ها و مراکز تحت پوشش بزرگ و پراکنده به بهترین نحو عمل می‌کند و در آن، بهترین فاکتورهای مدل توزیع شده(مجازی) و مدل متمرکز ترکیب شود[۱۱]. میزان کنترل تیم بر اعمال خود و محدوده عملکردش را می‌توان به سه سطح اختیارات کامل، اختیارات اشتراکی و بدون اختیار تقسیم نمود. CSIRTها در ابتدای شکل‌گیری، فاقد اختیار و اغلب از نوع ملی، هماهنگ‌کننده، تحقیقاتی و دانشگاهی بودند. اما هنگامی که CSIRTهای محلی، نظامی، تجاری، اطلاعات- ارتباطاتی و مالی- بانکی شکل گرفتند، برای انجام وظایف خود به اختیارات بیشتری نیاز داشتند. امروزه اکثر آنها دارای اقتدار کامل یا اقتدار مشارکتی هستند [۸].

برخی از تیم‌های CSIRT در بخش‌های IT، امنیت، بازرسی یا ممیزی قرار دارند. برخی تیم‌ها بسته به چارت سازمانی ممکن است جایگاه مستقل نیز داشته باشد. شخصی که CSIRT موظف به گزارش‌دهی به او است، به جایگاه سازمانی تیم بستگی دارد. CSIRTها ممکن است موظف به ارائه گزارشات به CIO، CSO، رئیس بازرسی یا رئیس ممیزی باشند[۸]. راهبردهای مختلف تامین بودجه CSIRTها شامل: دریافت حق عضویت از اعضا (مانند AusCERT)، خدمات دولتی (مانند FedCIRC)، خدمات قراردادی یا ارائه سرویس در ازای وجه (مانند CanCERT)، خدمات تحقیقاتی یا دانشگاهی (مانند CERT-NL حمایتی شبکه‌های تحقیقاتی SURFnet)، سرمایه‌گذاری سازمان بالادستی (مانند MCI WorldCom) و ترکیبی از موارد فوق (مانند CERT/CC) می‌باشد. در عین حال، اکثر CSIRTها (۵۵٪) هزینه‌های خود را از سازمان بالادستی دریافت می‌کنند و تعداد کمی از آنها (۱۰٪) در ازای ارائه سرویس، پشتیبانی می‌شوند [۸].

۳. مدیریت حوادث امنیتی رایانه‌ای

رسیدگی به حوادث جزئی، از فعالیت‌های CSIRT می‌باشد، اما در واقع، فعالیت‌های CSIRT، مجموعه بزرگتری را دربر می‌گیرد که به آن مدیریت حادثه اطلاق می‌شود. رسیدگی حادثه، یک سرویس پاسخ‌گویانه است که همه فرآیندها و اعمال مرتبط با رسیدگی رویدادها و نشانه‌ها را دربر می‌گیرد. این توابع شامل مراحل تشخیص و گزارش (مرحله دریافت و بازبینی اطلاعات رویدادها، گزارشات حادثه و هشدارها)، تریاژ (اعمالی که در رابطه با دسته‌بندی، اولویت‌گذاری، تعیین رویدادها و حوادث می باشد)، تحلیل (تلاش در جهت اینکه چه اتفاقی افتاده است، چه تاثیرات، تهدیدات، خرابی‌هایی به‌وجود آمده است؟ چه اقداماتی جهت تخفیف، ترمیم و بازیابی باید صورت پذیرد؟ این مرحله می تواند شناسایی تهدیدات جدید که ممکن است روی زیرساختار تاثیر بگذارند را در برگیرد) و پاسخ‌گویی به حادثه (شامل رفع یا تخفیف حادثه، هماهنگی و انتشار اطلاعات و به‌کارگیری راهبردهای متعاقب برای جلوگیری از وقوع مجدد حادثه) می‌باشد. پاسخ به حادثه، آخرین فرآیند از مراحل رسیدگی به حادثه است و مدیریت حادثه، شامل گستره وسیع‌تری از سرویس‌ها و توابع مثل رسیدگی به آسیب‌پذیری‌ها و کدهای آسیب‌رسان، آموزش، هشدارهای امنیتی و دیگر سرویس‌های مدیریت حادثه است که می‌تواند توسط CSIRT اجرا شود[۵]. فرآیند پاسخ‌گویی به یک حادثه رایانه‌ای، دارای مراحل مختلفی است که شامل آماده‌سازی، تشخیص و بررسی، محدودسازی، ریشه‌کنی و ترمیم و نیز فعالیت‌ها و پشتیبانی‌های بعد از رفع کامل حادثه می‌باشد [۴].

۴. اقدامات ایجاد CSIRT

اقدامات سطح بالایی که برای طرح‌ریزی و پیاده‌سازی CSIRTها و به‌عنوان نقطه شروع طراحی آنها نیاز است، توسط CERT/CC ارائه شده است:

- شناسایی ذی‌نفعان[۲] و شرکای ایجاد CSIRT
- حصول پشتیبانی مدیران
- توسعه طرح پروژه
- جمع‌آوری اطلاعات (برگزاری جلسات گفتگو با مسئولان برای تعیین نیازها و احتیاجات سازمان، دارایی‌های مهم، نوع حوادث سازمان و منابع موجود برای استخراج اطلاعات)
- شناسایی محدوده عملکرد
- تعریف ماموریت[۳]
- پرسنلی و آموزش، هزینه تجهیزات، توسعه، پیکربندی و نگهداری از ابزارهای امنیتی، برنامه‌های کاربردی و فراساختارها برای پیش‌گیری از وقوع حوادث، تعیین مدل درآمدزایی و مدل پرداخت وجه، تعیین تعرفه خدمات ارائه شده توسط CSIRT به متقاضیان خارج سازمان)

1- Computer Emergency Response Team

2– Stakeholders
3- Mission

- حدود و سطح سرویس‌ها (فرآیند تحویل سرویس‌ها شامل ساعات عملیات، شیوه‌های ارتباط، انتشار اطلاعات، تصمیم گیری در خصوص نحوه بازاریابی سرویس‌ها)
- تعیین جایگاه، مدل سازمانی، اختیارات و ساختار گزارش‌دهی (ایجاد چارت سازمانی، ساختار گزارش‌دهی به سازمان‌های دیگر و یا نهادهای سطح بالاتر)
- تعیین منابع مورد نیاز شامل نیروی انسانی، تجهیزات و زیرساخت‌های سازمان (ابزارها و زیرساختار شبکه برای تشخیص، آنالیز و پاسخ‌گویی به حوادث، تعریف فرآیندی برای جمع آوری، ثبت، پیگیری و بایگانی اطلاعات، توصیف شغل‌ها[1] شامل دانش‌ها، مهارت‌ها و توانایی‌ها[2](KSAs) برای هر جایگاه CSIRT، ایجاد یک طرح آموزش در تخصص‌های منحصر به فرد برای پرسنل)
- تعریف تعاملات و واسط‌ها (چگونگی جریان اطلاعات بین نهادها، تعریف روش‌هایی برای انتشار اطلاعات)
- تعریف نقش‌ها، مسئولیت‌ها و اختیارت متناظر
- مستندسازی جریان کاری
- توسعه سیاست‌ها و رویه‌های متناظر
- ایجاد یک طرح پیاده‌سازی و بازخورد تقاضا
- اعلان فعالیت رسمی CSIRT
- تعریف روش‌هایی برای ارزیابی کارایی
- داشتن پشتیبان[3] برای هر عنصرCSIRT [۲].

۵. مدل‌سازیCSIRT شرکت مخابرات استان‌ها

۱.۵. نیازسنجی

در شرکت مخابرات استان، حفظ امنیت و پاسخ‌گویی به مسائل امنیتی در حوزه شبکه‌های رایانه، به عهده اداره فناوری اطلاعات است که این وظیفه، به‌صورت مقطعی احیا شده و فقط در جهت رفع اشکالات و خسارات وارده به سبب رخداد امنیتی ایفای نقش می‌نمایند. نتایج نیازسنجی که با برگزاری نشست با مدیران شرکت مخابرات استان در خصوص مشکلات و انتظارات بخش امنیت رایانه‌ای این شرکت حاصل شده است، به شرح زیر می‌باشد:

- تشکیل واحدی متمرکز و مستقل، متولی امور امنیت فضای تولید و تبادل اطلاعات (افتا) شرکت و مجری دستورالعمل‌های اجرایی حراست فناوری اطلاعات.
- تشکیل شورای راهبردی افتا، متشکل از حوزه‌های مرتبط و تعیین اهداف، راهبردها و سیاست‌های شرکت در این حوزه.
- پاسخ‌گویی و مهار حوادث امنیت رایانه‌ای در کم ترین زمان ممکن و حداقل خسارات، استمرار فعالیت‌ها و ارائه سرویس‌ها.
- پیش‌گیری از وقوع حوادث با امن‌سازی سامانه‌ها، ایجاد آمادگی بیشتر و افزایش قدرت پیش‌بینی حملات امنیتی.
- طرح تحلیل خطرات و تحلیل شکاف و ارزیابی مداوم وضعیت شبکه، ترسیم وضعیت ایده‌آل و تدوین راهبرد رسیدن به آن.
- تربیت نیروی متخصص و خبره در زمینه امنیت فضای تبادل اطلاعات و ارتقاء سطح مهارت‌های رایانه‌ای کاربران و ارتقاء فرهنگ سازمانی در این زمینه.
- اطلاع‌رسانی و هشدار انواع آسیب‌پذیری‌های امنیتی.
- ارائه گزارش‌های موردی و دوره‌ای از اقدامات حفاظتی و امنیتی، نوع، شدت و تبعات رخدادهای امنیت رایانه‌ای، آسیب‌پذیری‌های نرم‌افزاری موجود در برنامه‌های کاربردی داخلی.
- تعیین دارایی‌های سازمان و ارزش‌گذاری آنها.
- ارزیابی ابزارهای امنیتی، برنامه های کاربردی شرکت و زیرساخت‌ها و تست دوره‌ای نفوذپذیری و امنیتی برنامه های کاربردی موجود و پیگیری نواقص احتمالی در صورت وجود.
- تهیه یک نسخه از اطلاعات پیکربندی تجهیزات بخش‌های مختلف شرکت، به‌روزرسانی آنها، نگهداری این مستندات در سامانه‌های پشتیبان‌گیری امن بر اساس استانداردها.

۲.۵. اعضای شورای راهبردی

اعضای این شورا شامل نمایندگانی از نهادهای امنیتی استان و یا نهادهای بالادستی است که CSIRT شرکت مخابرات استان برای ارائه خدمات قراردادی و سرویس‌های تعرفه‌ای، نیاز به هماهنگی با آنها دارد. مدیرکل اطلاعات استان، معاونت سیاسی- امنیتی استانداری (ریاست کارگروه امنیت فضای سایبر استان)، معاونت پشتیبانی و منابع انسانی استانداری (دفتر فناوری اطلاعات استانداری این معاونت، وظیفه هماهنگی ارتباط با ادارات دولتی و شرکت های خصوصی و نیز ارتباط با شبکه دولت را به عهده دارد)، مدیر کل سازمان تنظیم مقررات و ارتباطات رادیویی منطقه (تعیین تعرفه و تبیین مقررات) و مدیر عامل شرکت مخابرات استان، اعضای شورای راهبری CSIRT شرکت مخابرات استان را تشکیل می‌دهند. نهادهای امنیتی استان که در شورای راهبری عضویت دارند، CSIRT شرکت مخابرات استان را در توسعه ذی‌نفعان، شرکا و سرویس‌گیرندگان خدمات امنیتی یاری نموده و CSIRT با ارائه گزارش‌های بازه‌ای، مقطعی و موردی به این نهادها و پیاده‌سازی سیاست‌های این شورا، در ارزیابی و ارتقای وضعیت امنیت فضای سایبر استان، ایفای نقش می‌نماید.

1– Jobs
2- knowledge ،skills ،and abilities (KSA)
3- backup

۳.۵. توسعه اعضا و ذی‌نفعان

توسعه نهادهای خارجی ذی‌نفع و عضو CSIRT شرکت مخابرات استان‌ها، از اهمیت بالایی برخوردار است. هر چند که مطابق نظرسنجی‌ها، سازمان‌های دولتی، مراکز تحقیقاتی، دانشگاه ها و شرکت‌های خصوصی در مرحله سرمایه‌گذاری برای ایجاد CSIRT تمایل زیادی نشان ندادند، ولی به جهت اهمیت بالای مسئله امنیت سامانه‌های اطلاعاتی و مقابله با رخدادهای رایانه‌ای و نیز افزایش روزافزون تهدیدات امنیت رایانه‌ای، قطعاً به‌صورت ثابت و یا موردی به دریافت سرویس‌های امنیت رایانه‌ای، با پرداخت حق عضویت، خواهند پرداخت.

۴.۵. عوامل درگیر در ایجاد

در شرکت مخابرات استان، مدیران (مدیرعامل، اعضای هیئت مدیره و معاونین)، اداره فناوری اطلاعات (واحدهای نرم افزار، سخت‌افزار، پرتال و شبکه)، اداره حراست (واحد حراست فیزیکی و واحد امنیت شبکه)، اداره داده (واحدهای سوییچ و انتقال) و بخش مالی (عضو مالی هیئت مدیره و مدیر مالی) در ایجاد CSIRT نقش دارند.

۵.۵. ساختار CSIRT

ساختار CSIRT که شامل ماموریت، نوع و محدوده عملکرد، بخش‌های مختلف و سرویس‌ها، میزان اختیارات تیم، جایگاه سازمانی، مدل سازمانی، راهبردهای تأمین بودجه، نیازمندی های زیرساختی و فنی، نوع و سطح تعاملات تیم با دیگران و روال‌های کاری است، شرح داده می‌شود.

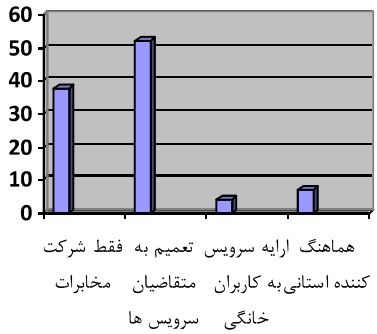
۱.۵.۵. تعریف ماموریت

ماموریت CSIRT شرکت مخابرات استان با نیازمندی‌های مطرح شده در جلسات گفتگو با مدیران و مسئولین فناوری تعیین شد که شامل:

- پاسخ‌گویی و مهار موثر حوادث رایانه‌ای
- پیش‌گیری از وقوع حوادث رایانه‌ای
- بهبود امنیت کلی سازمان، شناسایی ریسک‌ها و تهدیدات
- راه‌اندازی بخش مانیتورینگ شبکه
- حفظ و حراست از منابع داده‌ای
- ارتقاء سطح دانش کاربران رایانه‌ای شرکت
- اطلاع‌رسانی در خصوص آسیب‌پذیری‌ها، بدافزارها و هشدارهای امنیت رایانه‌ای
- توسعه ذی‌نفعان خارجی، ارائه سرویس‌های امنیتی به متقاضیان با دریافت تعرفه
- پشتیبانی و ارتقای سطح امنیت فضای سایبر رایانه‌ای استان (در صورت حمایت نهادهای امنیتی و دولت).

۲.۵.۵. نوع CSIRT و محدوده عملکرد

نتایج حاصل نظرسنجی انجام شده از مدیران شرکت مخابرات استان در خصوص محدوده عملکرد CSIRT، در نمودار ۱ ارائه شده است:



نمودار ۱. محدوده عملکرد CSIRT (بر حسب درصد)

بنابراین، نوع CSIRT، ترکیبی از انواع داخلی و ارائه‌دهنده سرویس‌های پاسخ‌گویی به حوادث می‌باشد. بدین معنی که اولویت آن سرویس‌دهی به محدوده داخلی شرکت مخابرات استان است و برای درآمدزایی، به متقاضیان خارجی نیز سرویس ارائه داده و ذی‌نفعان خود را توسعه می‌دهد.

CSIRT شرکت مخابرات، قابلیت تبدیل شدن به CERT هماهنگ‌کننده استانی را نیز دارد. با وجودی که نهادهای دولتی در این وظیفه ارجح‌ترند، اما مخابرات استان‌ها به‌علت نقش مدیریت ترافیک شبکه‌های استان و نیروهای فنی، می‌تواند با حمایت دولت و نهادهای امنیتی به‌عنوان CERT استانی ایفای نقش کند. محدوده عملکرد این CSIRT، علاوه‌بر شرکت مخابرات استان، به خارج شرکت خصوصاً به متقاضیان سرویس‌های امنیت شبکه دولتی، خصوصی و دانشگاه‌ها تعمیم می‌یابد.

۳.۵.۵. بخش‌های مختلف CSIRT و سرویس‌های ارائه شده توسط هر بخش

با توجه به ماموریت‌های CSIRT حاصل از نظرسنجی، وجود پنج بخش ذیل ضروری است. علاوه بر این، با توجه به جدول ۱، تقسیم‌بندی سرویس‌های ارائه شده توسط هر بخش نیز در ادامه انجام می‌شود:

- بخش عملیات فنی، مهار حوادث و هماهنگی پاسخ: سرویس‌های پاسخ به حادثه، پاسخ به کدهای آسیب‌رسان، پاسخ به آسیب‌پذیری، هماهنگی پاسخ به حادثه، هماهنگی پاسخ به کدهای آسیب‌رسان، هماهنگی پاسخ به آسیب‌پذیری.
- بخش پژوهش، آموزش و تولید محتوا: سرویس‌های رایزنی‌های امنیتی، رصد فناوری، تعلیم و آموزش، آگاهی‌رسانی و هوشیارسازی، انتشار اطلاعات مرتبط با امنیت.
- بخش تحلیل فنی و ارزیابی: سرویس‌های تحلیل حادثه، تحلیل کدهای آسیب‌رسان، تحلیل آسیب‌پذیری، تشخیص نفوذ، تحلیل مخاطرات، طرح‌ریزی ترمیم حادثه و تداوم فعالیت‌های تجاری، بازرسی امنیتی شبکه و نرم‌افزارهای داخلی.
- بخش پشتیبانی، ایمن‌سازی و نگهداری: سرویس‌های توسعه ابزارهای امنیتی، نگهداری از ابزارهای امنیتی، پیکربندی ابزارهای امنیتی و فراساختار.
- بخش امور متقاضیان: سرویس توافقنامه‌های ارائه سرویس.

کلیه این سرویس‌ها در محدوده عملکرد CSIRT مخابرات استان ارائه می‌شوند؛ برای مثال، در تحلیل آسیب‌پذیری، شبکه و برنامه‌های کاربردی محدوده داخلی شرکت/ مشترکین، CSIRT هدف است.

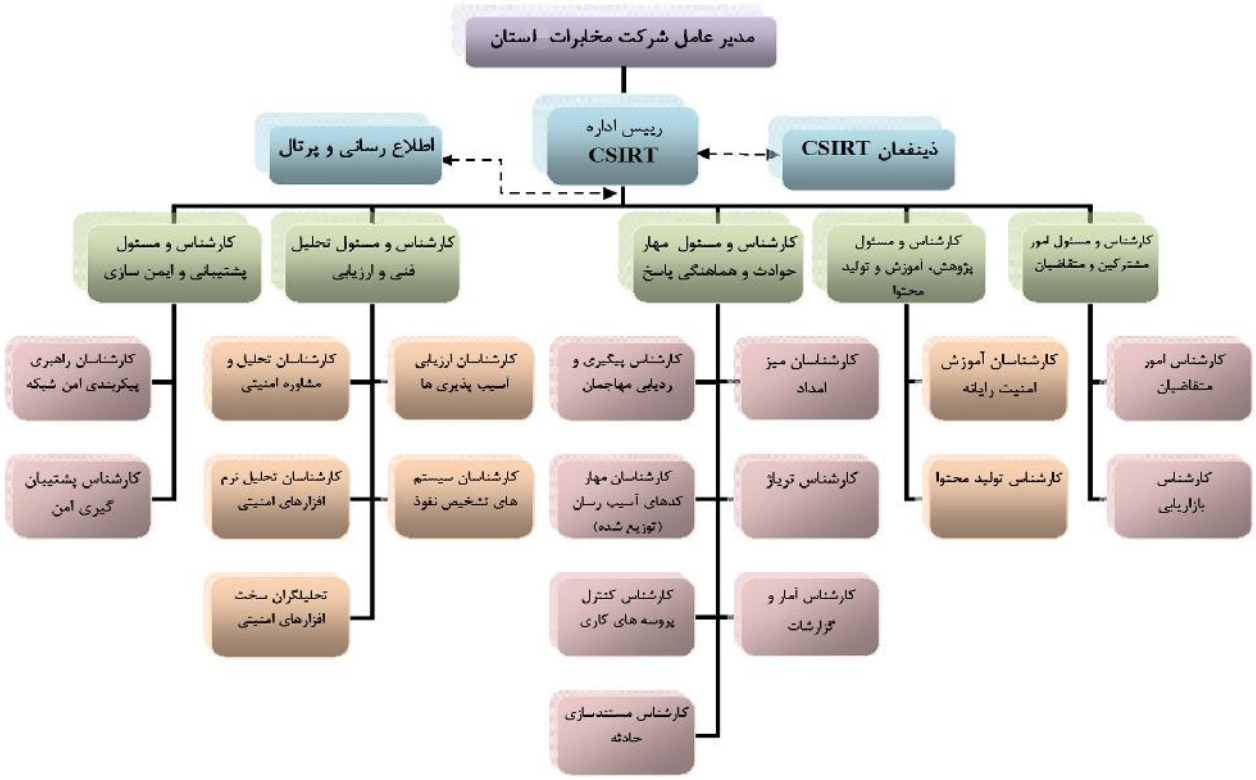
۴.۵.۵. جایگاه سازمانی

مطابق نظرسنجی از مدیران شرکت مخابرات استان، با توجه به نقش‌ها و مسئولیت‌های متنوعی که می‌بایست بر مبنای ماموریت، محدوده عملکرد و سرویس‌های CSIRT منظور شود، CSIRT باید جایگاه سازمانی مستقلی در ساختار سازمانی داشته باشد.

ولی از لحاظ موقیت فیزیکی، به‌علت تعاملات زیاد با اداره فناوری، می‌تواند در ساختمان IT مستقر شود. مدیر اجرایی CSIRT، موظف به ارائه گزارش به مدیر فناوری اطلاعات (CIO) و رییس امنیت شبکه حراست (CSO) می‌باشد.

همچنین برای جلوگیری از هم‌پوشانی وظایف، پیشنهاد می شود بخش‌های با کارکردهای امنیت رایانه‌ای موجود (واحد امنیت شبکه در اداره فناوری اطلاعات) در CSIRT ادغام شوند. البته مسئولیت‌های مختلف اداره فناوری اطلاعات که شامل نگهداری تجهیزات سخت‌افزاری شرکت (واحد سخت افزار)، نگهداری نرم‌افزارهای کاربردی (واحد نرم‌افزار) و نگهداری پرتال است، با استقرار CSIRT همچنان برقرار است و به‌جز در بحث امنیت رایانه‌ای مثل مبارزه با کدهای آسیب‌رسان، مهار احتمالی رخدادهای رایانه‌ای و اجرای طرح ایمن‌سازی شبکه، همپوشانی وظایف ندارند.

در شکل ۱، جایگاه CSIRT، بخش‌های مختلف آن و تخصص‌های



شکل۱. ساختار سازمانی CSIRT شرکت مخابرات استان و چارت سازمان

نیروی انسانی مورد نیاز هر بخش نشان داده شده است که این تخصص‌ها با توجه به سرویس‌هایی که توسط هر بخش می بایست ارائه شود، مشخص گردیده است.

۵.۵.۵. مدل سازمانی، شیوه گزارش‌گیری و تریاژ

نتایج نشستی که با مسئولین IT شرکت مخابرات برگزار گردید، حاکی از آن است که کلیه تجهیزات ارائه سرویس و منابع اطلاعاتی شرکت، به‌صورت متمرکز در ساختمان IT مستقر بوده و به صورت مرکزی مدیریت می‌شود و اغلب حوادث مهمی که تاکنون در شرکت مخابرات استان رخ داده است، پیرامون سایت IT و سرویس‌گرهای این حوزه می‌باشد. از طرفی، شبکه WAN شرکت، در سطح مراکز مخابراتی استان پراکنده‌اند و در این بخش‌های شبکه، حوادثی چون انتشار بدافزارها، استفاده‌های نامناسب از شبکه و اینترنت رخ می‌دهد. بنابراین، دو مدل متمرکز و یا ترکیبی (توزیع شده و متمرکز) برای CSIRT شرکت مخابرات قابل بررسی است که در ادامه خصوصیات این دو مدل مورد بررسی قرار می‌گیرد. مدل متمرکز که اغلب برای سازمان‌های متمرکز و کوچک پیشنهاد می‌شود، پاسخ‌گو به حوادثی است که در سایت‌های پراکنده و دوردست رخ می‌دهد و با اتلاف زمان همراه است. علاوه بر این، CSIRT، فاقد واحدهای عملیاتی جدا و مجزا بوده و نیز هماهنگی و اطمینان از پاسخ های سازگار و صحیح، در سطح محلی مشکل است. شماری از ویژگی‌های مدل ترکیبی شامل موارد ذیل است:

- تشکیل بخش متمرکز به‌صورت هسته‌ای پایدار از افراد حرفه ای تمام وقت
- توزیع تعدادی از کارمندان در موقعیت‌های استراتژیک سازمان و دیگر شهرستان‌ها
- جمع‌آوری، ترکیب و پیگیری تمامی گزارش‌ها توسط اعضای تیم مرکزی
- تحلیل سطح بالا و تدوین راهبردهای مهار رخدادها توسط تیم مرکزی
- پیاده‌سازی راهبردهای تدوین شده در هسته مرکزی، توسط اعضای پراکنده تیم
- پاسخ‌گویی سریع‌تر به رخدادها توسط اعضای توزیع شده تیم در سطح شهرستان‌ها
- انتقال مهارت و دانش به حوزه‌های مسئولیت، توسط اعضای توزیع شده تیم در سطح شهرستان‌ها

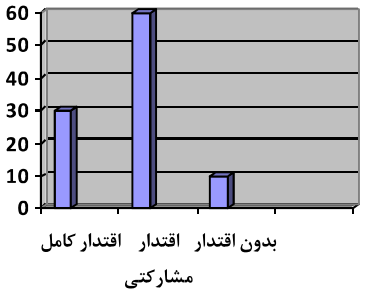
بنابراین، با توجه به ساختار شرکت مخابرات استان، در CSIRT، مدل سازمانی ترکیبی استفاده خواهد شد که تمامی گزارشات و درخواست‌ها وارد دفتر مرکزی می‌شوند و در آنجا رده‌بندی و اولویت‌گذاری (تریاژ) شده و انجام اقدامات پاسخ گویی و اجرای رویه‌های تدوین شده توسط تیم متمرکز، به تیم توزیع شده واگذار می‌شود.

۶.۵.۵. راهبردهای تامین بودجه

در ایران، ماهر به‌عنوان هماهنگ‌کننده دولتی و آپا به عنوان CERT تحقیقاتی- دانشگاهی، به‌ترتیب توسط دولت و مخابرات پشتیبانی می‌شوند. با توجه به اینکه شرکت مخابرات ایران از تجهیز و راه‌اندازی هشت مرکز تخصصی در هشت دانشگاه کشور حمایت نموده است، حمایت از تجهیز و راه اندازی CSIRT شرکت مخابرات استان‌ها چندان دور از انتظار نیست. پس از مرحله راه‌اندازی، CSIRT شرکت مخابرات استان‌ها، با توسعه اعضا، دریافت حق عضویت از آنها، ارائه خدمات مشاوره و سرویس‌های امنیت شبکه به متقاضیان خارج سازمان، به درآمدزایی و تامین هزینه‌های جاری خود خواهند پرداخت.

۷.۵.۵. اقتدار و میزان اختیارات

نتایج نشست با مدیران شرکت مخابرات استان در خصوص میزان اختیارات CSIRT در نمودار ۲ ارائه شده است.



نمودار ۲. اقتدار و میزان اختیارات CSIRT (بر حسب درصد)

استدلال اکثر مدیران شرکت مخابرات استان این بود که اگر CSIRT فاقد اختیارات اجرایی باشد و تنها توصیه‌ها و مستندات امنیتی را در شرکت منتشر کند، نقش آن تنها به هشداردهی محدود شده و مخاطبان ممکن است هشدارها را مهم تلقی ننموده و مانع عملیات اجرایی CSIRT شوند. از طرفی، CSIRT همانند کلیه ادارات مشابه مثل فناوری اطلاعات، نمی‌تواند دارای اقتدار کامل در تصمیم‌گیری و اجرا باشد و کلیه این برنامه‌ها و راهبرد، باید به تایید مدیران رده بالاتر برسد. بنابراین، CSIRT شرکت مخابرات استان، باید اختیار کاملی در تحلیل رخدادها و آسیب‌پذیری‌ها داشته و برای پاسخ‌گویی به حادثه و رفع مشکل، دارای اختیار اشتراکی باشد.

برای حمایت بیشتر از اعضاء توزیع شده، تیم مدیران شهرستان‌ها نیز باید در جریان هر اقدامی در حوزه کاری خود، قرار گیرند. CSIRT، همچنین باید مسئول بازبینی و تحلیل سامانه‌های تشخیص مزاحمت یا سایر ورودهای ثبت شده به شبکه، سامانه یا برنامه‌ها نیز باشد.

۸.۵.۵. نیازمندی‌های زیرساختی و فنی

نیازمندی‌های زیرساختی و فنی CSIRT مخابرات استان، شامل موارد ذیل می‌باشد:

۱) سازوکارهای ارتباطی چون تلفن و فکس

۲) تجهیز سایت CSIRT مطابق استانداردها:

- سامانه برق اضطراری، استفاده از دوربین‌های پایش و مقاوم‌سازی سخت‌افزاری
- امنیت فیزیکی (سامانه کنترل ورود و خروج افراد)
- لپ‌تاپ‌ها، انواع رسانه‌ها، ابزارهای فشرده‌سازی، چاپگر جابه‌جا شونده
- لوازم جمع‌آوری مدارک، شامل دوربین‌های دیجیتالی، ثبت کننده‌های صوتی و محفظه‌های ذخیره‌سازی جهت نگه‌داری مدارک حادثه
- نرم‌افزارهای لازم، تصاویر پشتیبان و وصله‌های امنیتی سامانه‌عامل و برنامه‌های کاربردی و داده‌ها

۳) عناصر زیرساختی شبکه:

- محدوده IP آدرس‌های معتبر برای اتصال به اینترنت
- دامنه اینترنتی وبی مانند (TCL-CERT)
- سامانه پست الکترونیک رمزگذاری شده به‌وسیله PGP[1] با قابلیت پالایش و جستجوی پیشرفته برای ارتباطات داخلی و خارجی مانند (@cert.tcl)
- پرتال امن دارای اطلاعات مهمی چون ماموریت تیم، هشدارها و توصیه‌های امنیتی، فرم‌های گزارش حادثه و آسیب‌پذیری، اطلاعات تماس و ...
- پیکربندی امن تجهیزات شبکه، مثل روترها برای غربالگری ترافیک با استفاده از لیست‌های کنترل دسترسی ACLها.
- فایروال‌های پیکربندی شده برای کنترل دسترسی[2] به/از شبکه و رویدادنگاری متمرکز.
- رایانه‌ها و سرویس‌دهنده‌ها (ابزارهای CSIRT، سرویس‌های وب، پست الکترونیک و DNS نیاز به سرور دارند).

۴) بستر سامانه عامل که به مهارت‌های اعضای تیم، نوع شبکه، محدوده عملکرد و هزینه‌ها بستگی دارد. به‌علت انعطاف‌پذیری و عمومیت استفاده در مخابرات استان، ویندوز به عنوان بستر انتخاب می‌شود، ولی با استفاده از نرم‌افزارهایی چون Virtual PC/ Server یا VMware، امکان نصب و اجرای آسان سامانه عامل به‌طور هم‌زمان وجود دارد.

۵) برنامه‌های کاربردی برای تیم‌های پاسخ به حادثه (AIRT)، قابلیت پیگیری حادثه را با پشتیبانی‌های تعبیه شده برای میز فرمان، جامع مدیریت حادثه، جستجوی مبتنی بر IP حوادث قبلی، قالب‌های پست الکترونیک و فرمت خروجی AIRT برای اشتراک داده‌های حادثه، فراهم می‌کند.

۶) فناوری‌ها و ابزارهای ارتباط بین CSIRTها، مانند CAIF، برای تبادل توصیه‌ها و هشدارهای امنیتی، IODEF، برای تبادل اطلاعات رسیدگی به حوادث امنیتی بین CSIRها و XIRL، برای تبادل حوادث امنیتی به‌نحوی ساخت‌یافته با تکنولوژی وب‌سرویس.

۷) استفاده از شبکه‌های خصوصی مجازی و ارتباطات نقطه به نقطه برای تبادل اطلاعات بین CSIRT شرکت مخابرات و دیگر تیم‌ها و نیز استفاده از PGP استاندارد رمزگذاری اطلاعات حساس، رمزهای عبور و پست الکترونیک بین CSIRTها در VPN تیم‌ها.

۸) ابزارهای بررسی‌های حقوقی که از جمله آنها می توان به TCT، برای Unix، EnCase Forensic و Helix برای Linux اشاره نمود. EnCase Forensic ابزار صنعتی استانداردی برای آشکارسازی، تحلیل و ارائه شواهد حقوقی شده است و به‌علت انعطاف‌پذیری و قوت، به‌وسیله بازرسان مجری قانون، دولت، شرکت‌های کوچک و بزرگ برای جستجو و بازیابی داده ها و شواهد حقوقی موجود روی دیسک‌های رایانه به‌کار می‌رود.

۹) توسعه سامانه‌های پشتیبان که آخرین خط دفاعی شبکه علیه حوادث امنیتی محسوب می‌شود. در Linux و Unix، ابزارهای tar، dump و dd و در ویندوز نیز ابزار dd برای پشتیبان‌گیری وجود دارد.

۱۰) توسعه ابزارها و نرم‌افزارهای امنیتی:

- نرم‌افزارهای دیواره آتش مبتنی بر شبکه/ میزبان و سرویس پروکسی.
- سامانه‌های تشخیص و جلوگیری از نفوذ (IDPS مبتنی بر شبکه و IDPS مبتنی بر میزبان برای سرورهای حیاتی).
- نرم‌افزارهای چک‌کننده جامعیت فایل.

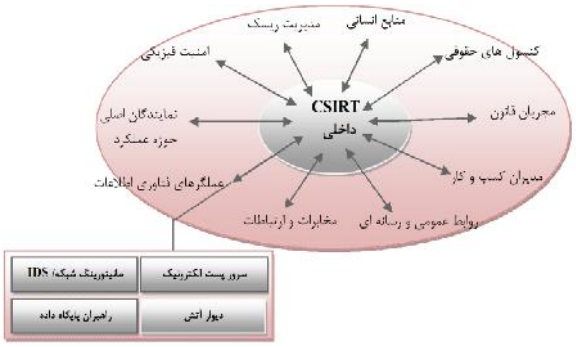
1- Pretty Good Privacy
2- Access Control List

- نرم‌افزار تحلیل رفتار شبکه.
- نرم‌افزار تشخیص و جلوگیری از مزاحمت‌های بی‌سیم.
- سرویس‌دهنده‌های واقعه‌نگاری متمرکز و نرم‌افزارهای مربوطه مثل sys log، security event، information software و IDPS مبتنی بر میزبان.
- نرم‌افزار پالایش اسپم در سرویس‌گرها و سرویس‌گیرنده‌های پست الکترونیک
- نرم‌افزار پالایش URL و محتوای وب
- نرم‌افزارهای پویش و حفاظت از ویروس، ابزارهای تشخیص و حذف جاسوس‌افزار [1]

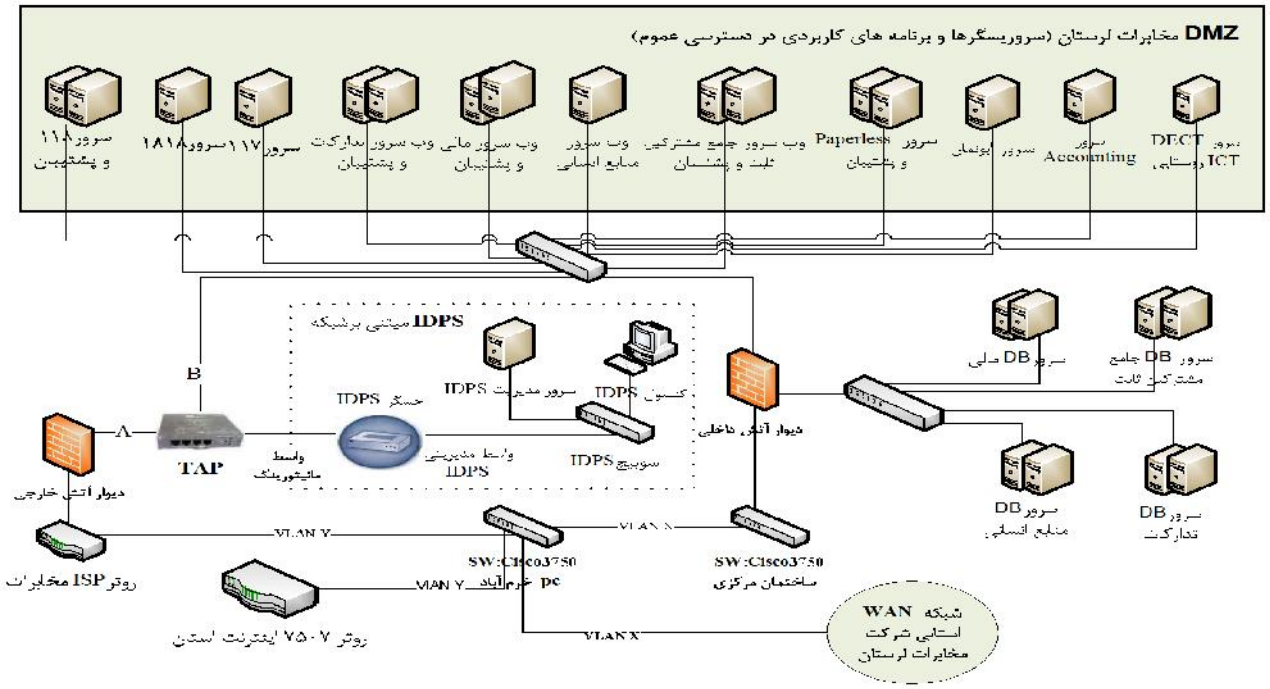
برای مثال، در شکل ۲ امن‌سازی دسترسی‌های عمومی به سرویس‌گرهای وب و برنامه‌های کاربردی شرکت مخابرات بررسی می‌گردد: درخواست‌های کاربران پس از عبور از روتر ISP مخابرات و فایروال خارجی، توسط واسط A، وارد TAP شده و از واسط B، به‌سمت DMZ حرکت می‌کند، اما یک رونوشت از جریان داده‌ای که از TAP عبور می‌کند، استراق سمع شده و به IDPS مبتنی بر شبکه برای تشخیص نفوذ احتمالی ارسال می گردد. در DMZ، کلیه سرویس‌گرهای وب و برنامه‌های کاربردی مختلف شرکت که در دسترس عموم قرار دارند، جای داده می‌شود. DMZ، ناحیه منطقی حفاظت شده‌ای است که خارج از شبکه داخلی شرکت قرار می‌گیرد تا دسترسی به سرویس‌های عمومی، موجب نفوذ به شبکه داخلی نشود. شبکه داخلی شرکت و سرویس‌گرهای پایگاه داده، پشت فایروال دوم قرار می‌گیرند. IDPS بین دو فایروال، نقش مهمی در تامین امنیت DMZ دارد و حسگر آن، برای مانیتور ترافیک ورودی به DMZ به‌کار می‌رود.

۹.۵.۵. تعاملات

شکل ۳، مدل مرجع CERT/CC برای تعاملات یک CSIRT داخلی را نشان می‌دهد. بر اساس این مدل مرجع، در جدول ۲ تعاملات CSIRT مخابرات استان، با توضیحات لازم ارائه شده است.



شکل ۳. مدل مرجع CERT/CC برای تعاملات یک CSIRT داخلی [۳]



شکل ۲. امن‌سازی دسترسی‌های عمومی به سرویس‌گرهای وب و برنامه‌های کاربردی شرکت مخابرات

1- Spyware

جدول۲. تطابق مدل مرجع CSIRT داخلی CERT/CC در شکل ۳ با CSIRT شرکت مخابرات استان

تعاملات یک CSIRT داخلی	نهاد مرتبط در شرکت مخابرات استان	توضیحات
امنیت فیزیکی	اداره حراست مخابرات استان	واحد امنیت فیزیکی اداره حراست مسئول تامین امنیت فیزیکی شرکت
نمایندگان اصلی محدوده عملکرد	در محدوده داخلی مخابرات استان، ادارات فناوری اطلاعات، دیتا و حراست در محدوده خارج شرکت، نمایندگان فناوری اطلاعات ادارات زیر مجموعه ۳۴ وزارتخانه استان، دانشگاه‌ها و شرکت‌های خصوصی استان	محدوده عملکرد CSIRT شرکت مخابرات استان، علاوه بر کل شرکت، شامل متقاضیان دریافت سرویس‌های امنیتی نیز می‌باشد. از ادارات دولتی که بحث امنیت اطلاعات برای آنها بسیار مهم است، می‌توان به دانشگاه‌ها، ثبت احوال، ثبت اسناد و املاک و بانک‌ها اشاره نمود.
متولیان فناوری اطلاعات سازمان	اداره دیتا و اداره فناوری اطلاعات مخابرات استان	اداره دیتا، وظیفه تامین زیرساخت‌ها (سامانه‌های انتقال، سوییچ‌ها، روترها، تجهیزات لایه دسترسی و تجمیع) و واگذاری سرویس‌های شبکه (شامل اینترنت، اینترانت، MPLS ، PTMP و ..) به کل مشترکین دولتی و خصوصی استان را به‌عهده دارد و اداره فناوری اطلاعات، سرویس‌گرهای وب و DB برنامه‌های کاربردی، سرویس‌گرهای ضدویروس، دیواره‌های آتش و ... را مدیریت می‌کند.
ارتباطات مخابراتی	شرکت مخابرات استان و زیرساخت	لینک‌های انتقال و ارتباط شبکه گسترده اینترنت مخابرات
ارتباط رسانه‌ای یا روابط عمومی	پرتال CSIRT و روابط عمومی مخابرات استان/ مشترکین CSIRT	دریافت رویدادها و گزارش حادثه، آموزش، اطلاع-رسانی رخداد امنیتی، هشدار و انتشار اطلاعات امنیت رایانه‌ای
مدیران تجاری	مدیران مالی و اقتصادی مخابرات استان	تدوین راهبرد جذب مشتری، بازاریابی و حمایت‌های مالی
کنسول‌های حقوقی	دادگستری استان و واحد حقوقی مخابرات استان یا مشترکین CSIRT	دادگستری استان، صدور احکام جرائم رایانه‌ای مرتبط با رخدادهای امنیت رایانه‌ای و واحد حقوقی مخابرات استان/ مشترکین، و CSIRT، وظیفه پیگیری صدور احکام، توسط دادگستری
مجریان قانون	نیروی انتظامی استان، واحد بازرسی و اداره حراست مخابرات استان یا مشترکین CSIRT	نیروی انتظامی استان، اجرای احکام جرائم رایانه‌ای مرتبط با رخدادهای امنیت رایانه‌ای و واحد بازرسی و اداره حراست مخابرات استان/ مشترکین CSIRT، پیگیری اجرای احکام، توسط نیروی انتظامی را به عهده دارد
منابع انسانی	کارمندان شرکت مخابرات استان و مشترکین دیتا	مشاهده رویداد، گزارش حوادث، ارائه نشانه‌ها و پیش‌روها و ارائه اطلاعات تکمیلی حین پاسخ‌گویی
مدیریت ریسک‌های امنیتی	اداره حراست، فناوری اطلاعات و بخش مالی	اداره حراست و IT برای ارزیابی آسیب‌پذیری‌های شبکه و نرم‌افزارها و میزان تهدید آن‌ها، بخش مالی برای شناخت دارایی‌ها، ارزش‌گذاری و تعیین ریسک آن‌ها

۱۰.۵.۵. روال کاری و گزارش‌دهی

شکل ۴، تعاملات CSIRT مخابرات استان هنگام رسیدگی به حادثه، جریانات کاری، گزارش‌دهی به سازمان‌های امنیتی و ارتباطات آن با CERTهای ملی را نشان می‌دهد.

در مرحله تشخیص، نشانه‌های رخداد توسط کاربران /TCL مشترکین دیتا (به‌وسیله تلفن، فکس، اپست الکترونیک و یا فرم‌های برخط موجود در پرتال (TCL-CERT به میز امداد مخصوص کاربران/ مشترکین، در بخش مرکزی تیم، گزارش می‌شود.

این نشانه‌ها، با گزارشات تجهیزات و نرم‌افزارهای آزمایشگاه-TCL CERT (مانند هشدارها و رویدادهای ثبت شده)/ وضعیت عمل‌گرها و اطلاعات سامانه‌های مانیتورینگ اداره دیتا (مانند قطع سامانه‌های انتقال و سوییچ) و اداره فناوری اطلاعات (مانند رویدادهای برنامه‌های کاربردی، سرویس‌گرها و اجزای شبکه)/ اطلاعات حاصل از مشاهدات عمومی و اطلاعات امنیتی موجود، ترکیب شده و پس از ثبت در پایگاه داده TCL-CERT، به مرحله تریاژ ارسال می‌شود.

در مرحله تریاژ، در صورتی که نشانه‌ها حاکی از آسیب‌پذیری یا حادثه امنیت رایانه‌ای نباشند، مسدود می‌گردند (مانند خرابی یا نویز ارتباط کابلی مشترکین یا کندی عمومی ترافیک) و در غیر این صورت، کلیه گزارشات جمع‌آوری، دسته‌بندی و اولویت‌دهی شده و پس از ثبت در پایگاه داده TCL-CERT، به مرحله تحلیل حادثه/ آسیب‌پذیری ارسال می‌شود.

مرحله تحلیل، توسط کارشناسان تحلیل حادثه/ آسیب‌پذیری بخش ارزیابی و تحلیل در آزمایشگاه TCL-CERT انجام می‌شود. تعیین نوع و تخمین شدت حادثه و نیز اولویت‌گذاری بر اساس حساسیت منابع آسیب‌دیده و تاثیرات بالقوه آن، از مهم‌ترین کارهایی است که در این مرحله صورت می‌گیرد. در صورت نیاز، اطلاعات تکمیلی از میز امداد کاربران یا مشترکین/ ادارات دیتا و فناوری اطلاعات/ NOC، زیرساخت/ ماهر یا دیگر CSIRT مخابرات استان‌ها گرفته می‌شود و با آنها هماهنگی لازم برای اجرای طرح پاسخ به‌عمل می‌آید.

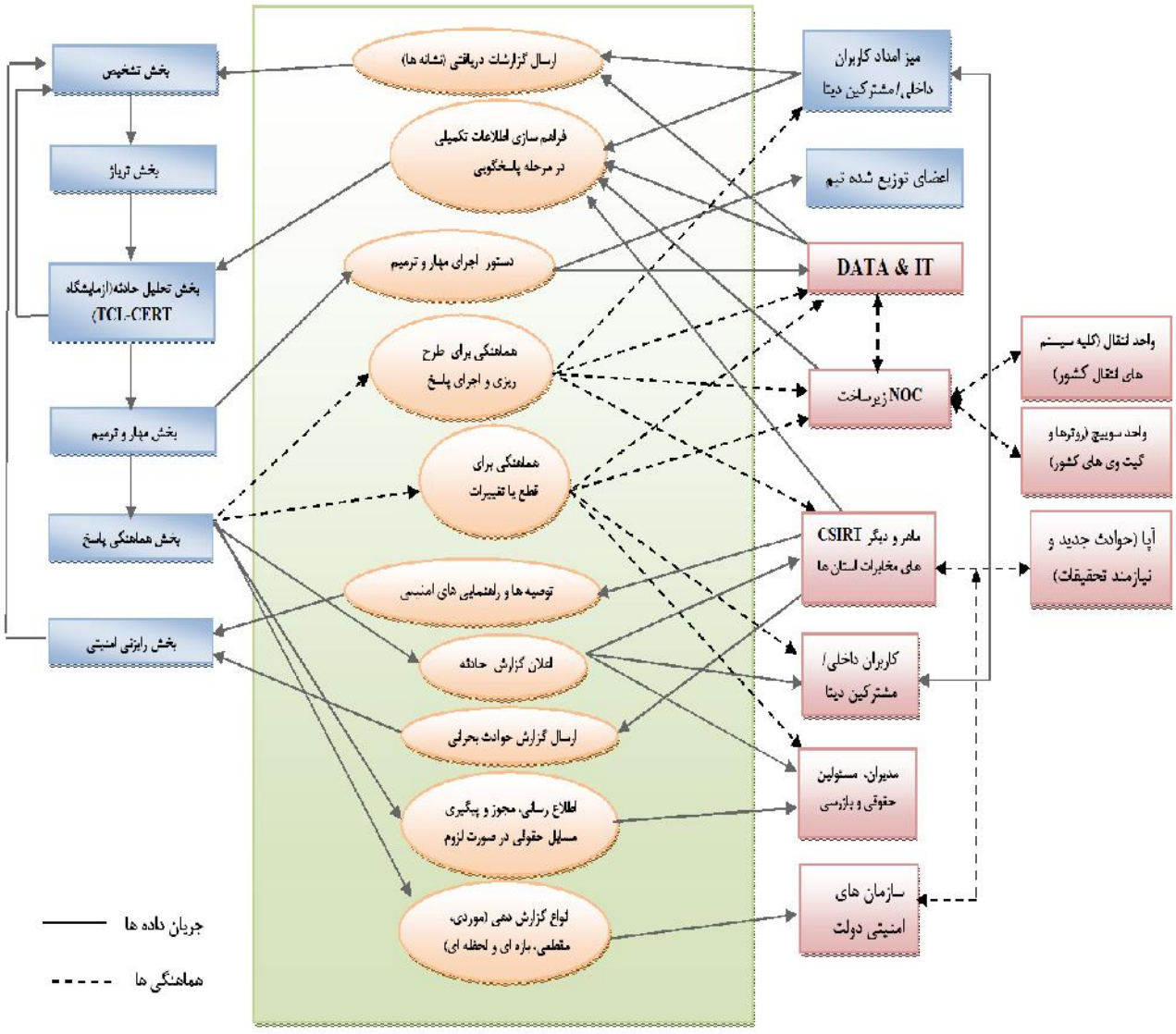
بخش هماهنگی پاسخ، در صورتی که اجرای پاسخ نیاز به قطع کاربر/ مشترک و یا اعمال تغییرات در ارتباط مربوطه داشته باشد، می‌بایست با مدیران و مسئولین مخابرات استان (برای حوادث داخلی)/ نماینده مشترک (برای حوادث خارج سازمان)/ اداره دیتا و فناوری اطلاعات/ NOC زیرساخت (در صورت لزوم)، هماهنگی های لازم را صورت دهد. اجرای پاسخ توسط اعضای تیم توزیع شده/ ادارات دیتا و فناوری اطلاعات انجام می‌شود.

گزارش حادثه به کاربر/ مشترک آلوده برای اطلاع ارسال شده و در صورتی که حادثه نیاز به پیگیری حقوقی داشته باشد، به واحد حقوقی مخابرات استان/ دادگستری استان ارجاع داده می‌شود.

۶. نتیجه‌گیری

رسیدگی به حوادث امنیت رایانه‌ای، تنها جزئی از مجموعه سرویس‌های CSIRT می‌باشد و CSIRT، علاوه بر مهار، در پیش-گیری از وقوع حوادث و ارتقاء سطح امنیت سازمان نیز ایفای نقش می‌کند. تفاوت‌های CSIRTها در اهداف، ماموریت‌ها و مقاصد آنها می‌باشد.

به‌منظور توسعه CSIRT، کسب حمایت مدیران شرکت و حصول منابع مالی از اهمیت بالایی برخوردار است. نتایج نشست با مدیران شرکت مخابرات استان، حاکی از آن است که وجود تیم‌های پاسخ‌گویی به حوادث رایانه‌ای در شرکت مخابرات استان، برای بحث امنیت داخلی شرکت یک ضرورت است.



شکل۴. دیاگرام جریان کاری CSIRT شرکت مخابرات و ارتباط با آپا و ماهر

در تصمیم‌گیری در خصوص ساختار و چارچوب عملیاتی CSIRT شرکت مخابرات استان‌ها که شامل ماموریت‌ها، اهداف و مقاصد، محدوده عملکرد، نوع و سطح سرویس‌ها، میزان اختیارات تیم، جایگاه در سازمان، نوع و سطح تعاملات با دیگران و نوع واسط ها، مدل سازمانی و راهبردهای تامین بودجه می‌باشد، مبنای کار یک CSIRT داخلی و ارائه‌دهنده سرویس‌های امنیتی است. تیم بر حسب نیاز و نوع حوادث، ممکن است با قسمت‌های خارجی مثل مسئولین امنیت فیزیکی، متولیان فناوری اطلاعات سازمان، بخش ارتباطات مخابراتی، ارتباط رسانه‌ای یا روابط عمومی، مدیران تجاری، کنسول‌های حقوقی، مجریان قانون، منابع انسانی و بخش مدیریت ریسک‌های امنیتی ارتباط برقرار کند.

۷. مراجع

[1] West-Brown. J, Stikvoort. M, Kossakowski. D, Peter. Audrey. K, Killcrece. G. Ruefle. R, Zajicek. M, Handbook for Computer Security Incident Response Teams (CSIRTs). U.S: Software Engineering Institute, Carnegie Mellon University, CMU/SEI-2003-HB-002. Available at http://www.sei.cmu.edu/reports/03hb002.pdf, April 2003.

[2] CERT/CC. Action List for Developing a Computer Security Incident Response Team (CSIRT). U.S: Carnegie Mellon University, Available at http://www.cert.org/csirts/action_list.html. October 2006.

[3] Killcrece. G, Ruefle. R, Creating and Managing Computer Security Incident Handling Teams(CSIRTs).U.S: Software Engineering Institute, Carnegie Mellon University, Available at http://www.first.org/conference/2008/papers/killcrece-georgia-slides.pdf, 2008.

[4] Scarfone. K, Grance. T, Masone. K, Computer Security Incident Handling Guide. U.S: Department of Commerce, National Institute of Standards and Technology, NIST SP 800-61, Available at http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf, March 2008.

[5] Alberts. C, Dorofee. A, Killcrece. G, Ruefle. R, Zajicek. M, Defining Incident Management Processes for CSIRTs: A Work in Progress. CMU/SEI-2004-TR-015,Available at www.sei.cmu.edu/reports/04tr015.pdf, October 2004.

[6] Stelvio. Bv, CSIRT Services. The Netherlands: PRESECURE Consulting GmbH Germany, 2002.

[7] CERT®/CC. Computer Security Incident Response Team FAQ. Available at www.cert.org/csirts/csirt_faq.html, Apr 2008.

[8] Killcrece. G, Kossakowski. K.P, Ruefle. R, Zajicek. M, State of the Practice of Computer Security Incident Response Teams (CSIRTs). US: Carnegie Mellon University, CMU/SEI-2003-TR-001. Available at www.cert.org/archive/pdf/03tr001.pdf, October 2003.

[9] IETF . "Extended Incident Handling (inch)", Available at http://www.ietf.org/html.charters/inch-charter.html, 2005.

[10] P. Timothy, "Creating and Managing an Incident Response Team for a Large Company", SANS Institute InfoSec Reading Room, Available at http://www.sans.org/reading_room/whitepapers/incident/creating-managing-incident-response-team-large-company_1821, 2007.

[11] Killcrece. G, Kossakowski. K. P, Ruefle. R, Zajicek. M, "Organizational Models for Computer Security Incident Response Teams (CSIRTs)" , CMU/SEI-2003-HB-001, Available at http://www.cert.org/archive/pdf/03hb001.pdf. December 2003

[12] Killcrece. G, "Steps for Creating National CSIRTs", CERT CSIRT Development Team, CERT® Coordination Center, Networked Systems Survivability Program, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA 15213-3890, August 2004.