فصلنامه علمی امنیت ملی

سال سیزدهم، شماره چهل و هشتم، تابستان ۱۴۰۲

مقاله چهارم از صفحات ۱۱۲-۸۷

# ارایه مدل ترکیبی تیم پاسخ‌گویی فوریتی رایانه‌ای مراکز دفاعی

**محمدرضا کریمی قهرودی**[۱]، رضا کشاورز[۲]، محمدرضا موحدی صفت[۳] و محمود صالح اصفهانی[٤]

**تاریخ دریافت: ۱۴۰۱/۰۵/۱۹** **تاریخ پذیرش: ۱۴۰۱/۰۷/۳۰**

## چکیده

امروزه با رشد و توسعه فناوری اطلاعات، زیرساخت‌ها و سامانه‌های اطلاعاتی مراکز دفاعی نیز بر بستر فناوری اطلاعات بنانهاده شده است؛ به‌طوری‌که در اثر غفلت و کوتاهی در مراقبت از شبکه، احتمال از دست رفتن اطلاعات و دارایی‌ها متصور خواهد بود؛ برای اینکه پاسخ‌گویی به رخدادهای پیش‌آمده در کمترین زمان ممکن صورت پذیرد، راه‌اندازی یک تیم پاسخ‌گویی رایانه‌ای در مراکز دفاعی امری ضروری است؛ به‌طوری‌که در یک بستر قابل‌اطمینان بتوان شبکه را کنترل نمود و حملات و نفوذهای غیرمجاز را تشخیص داد و در کم‌ترین زمان ممکن با ارتباط بهینه بین اجزاء، سرعت پاسخ‌گویی را بالا برد؛ از طرفی حفظ سلسله مراتبی و چابکی و استفاده از سامانه‌های بلادرنگ از تمایزات این تیم نسبت به تیم‌های غیر دفاعی است؛ در این تحقیق با اتکا به روش کتابخانه‌ای، داده‌های موردنیاز استخراج شد و با نظر خبرگان حوزه دفاع سایبری، سوالاتی تنظیم و در بین ٦٥ نفر از خبرگان جامعه هدف توزیع گردید؛ نتایج این تحلیل با استفاده از نرم‌افزار اس‌پی‌اس‌اس، به‌عنوان نتایج تحقیق ارائه شد و برای مرکز فرماندهی، مدل هماهنگ‌کننده و برای لایه‌های پایین‌تر، مدل ترکیبی (توزیع‌شده و متمرکز) پیشنهاد شد؛ همچنین نحوه تعاملات، خدمات و سرویس‌ها، میزان اختیارات، روش گزارش‌گیری و چارت سازمانی ارائه گردید.

**کلیدواژه‌ها:** مدل، رخداد، تیم پاسخ‌گویی فوریتی رایانه‌ای، مراکز دفاعی، سلسله مراتبی.

۱- عضو هیات علمی دانشگاه مالک اشتر، (نویسنده مسئول)، M_karimi@mut.ac.ir..

۲- دانش‌آموخته مقطع دکتری دانشگاه عالی دفاع ملی.

۳- دانشیار و عضو هیات علمی دانشگاه عالی دفاع ملی.

٤- استادیار و عضو هیات علمی دانشگاه امام حسین (ع).

## ۱- مقدمه و بیانیه مسئله

با گسترش فن‌آوری اطلاعات و ارتباطات در همه ابعاد و حوزه‌ها، بسیاری از دارایی‌های مهم سازمان‌ها که بعضاً دارایی‌های حیاتی هم می‌باشند در بستر شبکه قرارگرفته‌اند. این دارایی‌ها همواره در معرض تهدیدات و آسیب‌پذیری‌های جدی قرار دارند. حملات رایانه‌ای در محیط شبکه مراکز دفاعی روزبه‌روز در حال افزایش هستند و ممکن است در یک بازه زمانی بسیار کوتاه، شبکه را دچار اختلال و آسیب نماید. در هنگام بروز مشکلات و تهدیدات امنیتی در یک سازمان لازم است که شیوه‌های پاسخ‌گویی مناسب در آن سازمان وجود داشته باشد. سرعت در تشخیص، تحلیل و پاسخ‌گویی یک مشکل امنیتی، میزان خطر و هزینه‌ترمیم را کاهش می‌دهد. تیم پاسخ‌گویی فوریتی به رخداد رایانه‌ای[۱]، یک تیم خدماتی است که مسئول دریافت، مرور و پاسخ‌گویی به گزارشات ارسالی و فعالیت‌های مربوط به مشکلات و رویدادهای رایانه‌ای است (پندو[۲]، ۲۰۱۶: ۱۳). درواقع تیم پاسخ‌گویی یک نقطه مرکزی برای گزارشات مرتبط با مشکلات امنیتی است که پس از بررسی اطلاعات واردشده، الگو و هدف فعالیت مخرب در آن شناسایی گردیده و عکس‌العمل مناسب نشان داده می‌شود. تیم پاسخ‌گویی می‌تواند با سایر تیم‌های پاسخ‌گویی به رخداد رایانه‌ای در خارج سازمان همکاری داشته باشد. این همکاری به اشتراک راهبردها در پاسخ‌گویی به حملات مشابه می‌انجامد و به‌عنوان یک هشداردهنده برای مشکلات بالقوه است (براون لی[۳]، ۲۰۱۸: ۲۱).

تأمین امنیت اطلاعات و زیرساخت در مراکز دفاعی در محیط امروزی که از شبکه‌های به‌هم پیوسته تشکیل‌شده، کاری مشکل است و با ورود هر محصول الکترونیکی و هر ابزار نفوذ این کار صعب، سخت‌تر نیز می‌شود. مدیران در مراکز دفاعی متوجه شده‌اند که یک راهکار امنیتی واحد برای تامین امنیت شبکه وجود ندارد؛ بلکه باید از راهبرد امنیتی چندلایه بهره گرفت که می‌تواند دفاع لایه به لایه یا دفاع در عمق باشد. یکی از لایه‌هایی که بیشتر سازمان‌ها در راهبرد امنیتی خود در نظر می‌گیرند، ایجاد یک تیم فوریتی برای پاسخ‌گویی به رخدادهای رایانه‌ای است (پییرجاکوبز[۴]، ۲۰۱۹: ۳). زمانی می‌توان از فضای سایبر به عنوان پیونددهنده زیرساخت‌های حیاتی کشور استفاده نمود که مسئله امنیت آن به‌طور کامل حل‌شده باشد، وجود هرگونه شکاف امنیتی در این فضا و همچنین در اجزایی که در این فضا عمل می‌نمایند، ضربات جبران‌ناپذیری را به کشور وارد خواهد کرد (صیاد و همکاران، ۱۳۹۹: ۱۲).

این تیم یک نقطه مرکزی برای گزارش مشکلات امنیتی است که پس از بررسی اطلاعات وارد شده، هدف و الگوی فعالیت مخرب را شناسایی کرده و بر اساس آن عکس‌العمل مناسب نشان داده می‌شود. تیم پاسخ‌گویی می‌تواند با بقیه تیم‌های پاسخ‌گویی به حوادث رایانه‌ای در خارج سازمان همکاری داشته باشد؛ این همکاری منجر به اشتراک راهبردها در پاسخ‌گویی به حملات مشابه شده و به عنوان یک هشداردهنده برای مشکلات بالقوه در نظرگرفته می‌شود، (پندو، ۲۰۱۶: ۱۹).در حال حاضر به دلیل عدم وجود یک استاندارد تعریف شده، این تیم اهداف، وظایف و ساختارهای متفاوتی دارند. افراد مشغول در بعضی تیم‌ها تنها به‌مرور اطلاعات ثبت‌شده از تشخیص نفوذ[۵] می‌پردازند،

---

۱- Computer Emergency Response Team (CERT).

۲- Penedo.

۳- Brownlee.

٤- Pierre Jacobs.

٥- Intrusion Detection.

درحالی‌که برخی دیگر به بازسازی و ترمیم[۱] سیستم‌ها، آموزش و اطلاع‌رسانی امنیتی، تحلیل آثار به‌جامانده از نفوذگرها[۲]، انتشار اخطاریه‌ها[۳] و هشدارهای[٤] امنیتی و انجام مشاوره و بازبینی امنیتی می‌پردازند.

ازاین‌رو دغدغه‌های اصلی برای طرح این مساله موارد زیر هستند:

- بر اساس مطالعات انجام شده، بیشتر مراکز دفاعی دارای مرجع مناسب و شیوه‌نامه منسجمی برای پاسخ‌گویی کارآمد به تهدیدات و رخدادهای رایانه‌ای نیستند؛
- برای مقابله با تهدیدات و پاسخ‌گویی به تهدیدات رایانه‌ای، تیم‌های امنیتی در مراکز دفاعی ایجاد شده است، اما با توجه به کارکرد و ساختار تیم پاسخ‌گویی، تیم‌های امنیتی قادر به ارایه خدمات موردنیاز برای مراکز دفاعی نیستند؛
- دارایی‌های مراکز دفاعی بر بستر سامانه‌های فناوری اطلاعات قرارگرفته‌اند و امنیت لازم با توجه به رشد تهدیدات در حوزه فناوری اطلاعات به میزان کافی وجود ندارد؛
- در عصر حاضر با گسترش فناوری اطلاعات شاهد افزایش دانش سازمان‌های مهاجم و هکرها هستیم و با گسترش دانش و ترفندها، تهدیدات پیچیده‌تر شده و تهدیدات به‌صورت شبکه‌ای شده‌اند و لذا برای پاسخ‌گویی مناسب به این تهدیدات نیاز به ساختار مناسب است؛
- کمبود شیوه مناسب و منسجم و نیز عدم وجود مرجع هماهنگ‌کننده واحدی در پاسخ‌گویی به تهدیدات رایانه‌ای در مراکز دفاعی، موجب افزایش آسیب‌پذیری در برابر تهدیدات شده و خسارات جبران‌ناپذیری ایجاد خواهد شد؛
- دغدغه اصلی از انجام این تحقیق، ارایه مدل مناسبی برای تیم پاسخ‌گویی به فوریت‌های رایانه‌ای در مراکز دفاعی است؛ به‌طوری‌که، مدل تعاملات، خدمات و سرویس‌ها، میران اختیار، روش پاسخ‌گویی و غیره در این تیم مشخص شود و در تصمیم‌سازی مدیران مراکز دفاعی بتواند کارگشا باشد.

## ۲- اهمیت تحقیق

مدل و نحوه ارتباطات در پاسخ‌گویی یک تیم، در شکل‌گیری ساختاری منسجم و هماهنگ جهت پاسخ‌گویی به تهدیدات رایانه‌ای در مراکز دفاعی موثر خواهد بود. این مدل می‌تواند جهت بهره‌برداری از ظرفیت‌های موجود به کار گرفته شود و روشی مناسب برای پاسخ‌گویی به تهدیدات رایانه‌ای است؛ از طرف دیگر، در صورت ترغیب تصمیم گیران مراکز دفاعی برای ایجاد تیم پاسخ‌گویی، شاهد افزایش انعطاف‌پذیری و آمادگی در برابر تهدیدات رایانه‌ای، کاهش خسارات و صدمات به زیرساخت‌ها، تجهیزات و سامانه‌ها، اطلاع از وضعیت امنیتی شبکه و سامانه‌های رایانه‌ای و شناسایی زودهنگام تهدیدات رایانه‌ای خواهیم بود.

---

۱- Recovery.

۲- Artifact.

۳- Alert.

٤- Warning.

## ۳- ضرورت تحقیق

با ایجاد یک ساختار سازمانی مناسب در برابر تهدیدات پیشرفته امروزی، یکی از کنترل‌کننده‌های لازم برای این امر محقق خواهد گردید. چنین شرایطی صیانت از زیرساخت‌های مراکز دفاعی را تأمین خواهد کرد. لذا در حالت کلی ازآنجایی که ضرورت انجام این تحقیق سلبی است، ضرورت آن به علت موارد زیر می‌باشد:

- ✓ کمبود واکاوی و بررسی مناسب برای ایجاد یک تیم مناسب برای پاسخ‌گویی فوریتی به تهدیدات رایانه‌ای؛
- ✓ کمبود مدل برای تیم پاسخ‌گویی به فوریت‌های رایانه‌ای در مراکز دفاعی، موجب کمبود انسجام در هماهنگی بین بخش‌های مختلف مراکز دفاعی در مواجهه با تهدیدات امنیتی خواهد شد؛
- ✓ کمبود فرآیندها و ساختارهای سازمانی برای مقابله با تهدیدات رایانه‌ای؛
- ✓ در صورت عدم توجه به شکل‌گیری این تیم، شاهد خسارات جبران‌ناپذیر ناشی از تهدیدات رایانه‌ای در شبکه سازمانی مراکز دفاعی خواهیم بود.

## ٤- هدف تحقیق

با توجه به اینکه تهدیدات رایانه‌ای به‌سرعت در حال گسترش و پیچیدگی بالا می‌باشند و نظر به اهمیت بسترهای موجود در زیرساخت‌های مراکز دفاعی و لزوم حراست از این زیرساخت‌ها و پاسخ‌گویی به تهدیدات موردنظر، نیاز است تا مدل ارتباطی و سرویس‌های لازم برای تیم پاسخ‌گویی مراکز دفاعی تهیه شود؛ هدف این تحقیق، ارائه مدلی جهت به‌کارگیری تیم پاسخ‌گویی مراکز دفاعی در برابر کاهش تهدیدات رایانه‌ای است و تلاش در راستای آگاهی بخشیدن و ارایه شناخت کافی به مخاطبان جهت پیاده‌سازی تیم پاسخ‌گویی و نیز روش به‌کارگیری تیم پاسخ‌گویی مراکز دفاعی و تاثیر ایجاد این ساختار بر کاهش تهدیدات رایانه‌ای در مراکز دفاعی است.

## ٥- سؤال تحقیق

سوال اصلی این تحقیق عبارت است از: مدل تیم پاسخ‌گویی به فوریت‌های رایانه‌ای در مراکز دفاعی شامل تعاملات، مدل پیاده‌سازی، سطح اختیارات، سرویس‌ها و خدمات اصلی و فرعی، روش گزارش‌گیری و ساختار کارکنان آن چگونه است؟

## ٦- پیشینه تحقیق

در فرآیند مطالعات پیشین، روش‌شناسی به‌عنوان قسمتی از یک چارچوب مدیریتی مناسب برای شناسایی و ارزیابی فرآیند موردنیاز است؛ به همین منظور در مقاله‌ای با عنوان "ارایه الگوی استقرار تیم پاسخ‌گویی فوریتی رایانه‌ای مراکز دفاعی"، روش پاسخ‌گویی به حوادث از دیدگاه‌های مرکز موسسه استاندارد و فناوری[1] و موسسه فوریتی امنیتی[2] و مرکز فوریتی رایانه‌ای ژاپن[3] را موردبررسی قرار داده است؛ همچنین تطبیق مدل‌های تیم پاسخ‌گویی در پاسخ‌گویی به حوادث، سرویس‌ها و ساختارهای پیشنهادی مراکز دفاعی، الگوی فرآیند نحوه مقابله تیم پاسخ‌گویی در مراکز دفاعی با یک رخداد و ارتباط بین مولفه‌ها در این مقاله بررسی‌شده و درنهایت مدل استقرار تیم پاسخ‌گویی

---

۱- NIST (National Institute of standard and technology).

۲ - SEI (Security Emergency Insitue).

۳- jappanices CERT (JPCERT).

مراکز دفاعی ارایه گردیده است (کشاورز، ۱۳۹۳: ۹۷). همچنین مقاله‌ای از نشریه‌ی آپای دانشگاه فردوسی مشهد، به بررسی انواع تیم‌های پاسخ‌گویی پرداخته و روش‌های مقابله با رخدادهای رایانه‌ای و بررسی نقاط قوت و ضعف انواع تیم پاسخ‌گویی را موردبررسی قرار داده است و این موارد از نقاط اشتراک این مقاله با موضوع موردتحقیق می‌باشد (طیرانی، ۱۳۹۵: ۲۳). پرداختن به خدمات تیم پاسخ‌گویی، خدمات مدیریت کیفیت امنیت و اندازه تیم و تعداد نفرات از دیگر موارد موردنیاز در مطالعه تیم پاسخ‌گویی می‌باشند که در مقاله‌ای دیگر به این مسأله پرداخته‌شده است (رشتی، ۱۳۸۸: ۱۲۳). مدیریت مخاطرات و آنالیز موقعیتی و مکانی از دیگر موارد مورد تفحص شده در نشریه سایبری طرح پاسخ‌گویی به فوریت‌های رایانه‌ای[۱] می‌باشند. همچنین معماری و اجزای لایه معماری تیم پاسخ‌گویی نیز به‌عنوان یکی از مهم‌ترین مؤلفه‌ها در بررسی یک تیم پاسخ‌گویی از سند سایبر ملی مورد استفاده قرارگرفته است (طرحی برای آینده ایمن سایبری[۲]، ۲۰۱۷).

## ۷-مبانی نظری تحقیق

### ۷-۱- رویدادها[۳] و رخدادهای رایانه‌ای[٤]

برای سازمان‌دهی قابلیت پاسخ‌گویی به حوادث رایانه‌ای چند جنبه مهم باید تعریف گردد: یکی از آن‌ها تعریف واژه حادثه است. هر اتفاق قابل‌مشاهده در یک سیستم یا شبکه یک رویداد است. یک رویداد مثلاً اتصال کاربر به فایل‌های مشترک و یا ارسال یک پست الکترونیک است. یک رویداد مضر دارای پیامد منفی است مثل طغیان بسته‌های شبکه، هنگ کردن سیستم، استفاده غیرمجاز از داده‌های حساس و غیره. رخداد امنیتی رایانه‌ای[۵] شامل تهدید حتمی به خط‌مشی امنیتی رایانه‌ای است. یک حادثه به دلایل فراوانی ممکن است اتفاق بیفتد؛ بنابراین ارایه یک‌رویه جامع با یک دستورالعمل مرحله‌به‌مرحله برای هر نوع حادثه‌ای غیرممکن است پس بهتر است به بحث در خصوص حوادث رایج پرداخته شود. طبقه‌بندی حوادث که در ادامه به آن ارائه شده یک دسته‌بندی اولیه می‌باشد:

**الف. از کار اندازی سرویس**[٦]: حمله‌ای که به استفاده‌های مجاز از شبکه‌ها، سیستم‌ها و برنامه‌های کاربردی آسیب می‌رساند و یا از آن‌ها جلوگیری می‌کند. هدف از این حملات، ایجاد اختلال در منابع و یا سرویس‌هایی است که کاربران قصد دست‌یابی و استفاده از آنان رادارند برای مثال در این حمله، مهاجم داده‌هایی به وب سرور می‌فرستد که منجر به آسیب آن می‌شود یا نفوذگر، از صدها رایانه خارجی برای فرستادن درخواست‌های پروتکل پیام کنترل اینترنتی[۷] به شبکه استفاده می‌کند که منجر به ازکارافتادن آن می‌شود.

---

۱- National Cyber Incident Response Plan.

۲- Blueprint for a Secure Cyber Future.

۳- Events.

٤- computer incident.

٥- computersecurity incident.

٦- Denial of Service(DOS).

۷- ICMP.

ب. **انتشار بدافزارها**: به یک ویروس، کرم، تروجان و دیگر کدهای آسیب‌رسان که یک رایانه را آلوده می‌کنند اطلاق می‌شود. برای مثال ممکن است سازمان از طرف یک فروشنده ضدویروس اخطاری دریافت کند مبنی بر این‌که ویروس جدیدی به‌سرعت از طریق پست الکترونیک در اینترنت پخش می‌شود. این ویروس از آسیب‌پذیری که هم‌اکنون در میزبان‌های سازمان وجود دارد، بهره می‌برد. ازاین‌رو انتظار می‌رود در زمان اندکی تعدادی از میزبان‌ها آلوده شوند.

ج. **دسترسی غیرمجاز**[۱]: هنگامی‌که شخصی دسترسی غیرمجاز فیزیکی و یا منطقی به شبکه، سیستم، برنامه کاربردی، داده‌ها و یا دیگر منابع فناوری اطلاعات را بدست می‌آورد. برای مثال مهاجم ابزاری را برای بدست آوردن دسترسی به رمز عبور سرور اجرا می‌کند و شخصی دسترسی مدیریتی غیرمجاز به سیستم و داده‌های حساس به دست می‌آورد.

د. **استفاده نامناسب**[۲]: زمانی که شخصی از استفاده مجاز از شبکه و یا هر جزء رایانه‌ای تخطی کند. کپی‌های غیرمجاز از نرم‌افزار و یا مثلاً تهدید افراد از طریق پست الکترونیک از این دسته محسوب می‌شوند.

ه. **حملات ترکیبی**[۳]: با تقسیم کردن حوادث به دسته‌های معین و ارائه راهنمایی‌هایی برای تشخیص، تحلیل و پاسخ‌گویی به هر یک از انواع حوادث می‌توان پاسخ‌گویی را به نحو موثرتری انجام داد. طبقه‌بندی کردن فقط با مشخص کردن نوع حادثه‌ای که گزارش‌شده است انجام نمی‌شود بلکه شامل تعیین رابطه حادثه با دیگر حوادث نیز هست. به‌عنوان‌مثال آیا این گزارش، یک گزارش تازه است یا بخشی از یک واقعه متداول و در حال پیشرفت است؟ آیا نوع این حمله مشخص است یا از یک نوع جدید است؟ اگر نمونه حادثه از قبل وجود نداشته باشد پس از طبقه‌بندی به رویه تعیین اولویت ارسال می‌شود (اسکارفن و همکاران[۴]، ۲۰۱۸: ۸).

### ۷-۲- برخی از سازمان‌های نقش‌آفرین برای ایجاد تیم پاسخ‌گویی فوریتی رایانه‌ای

با توجه به اسناد بالادستی و شرح خدمات سازمان‌ها، بیشترین همکاری‌ها و نقش‌آفرینی‌ها با تیم پاسخ‌گویی با مرکز ماهر، مرکز ملی فضای مجازی و پلیس فتا است که به‌صورت زیر آمده است:

- مرکز ماهر:

مرکز مدیریت امداد و هماهنگی رخدادهای رایانه‌ای «ماهر»، یک نقطه کانونی در سطح وزارت ارتباطات و فناوری اطلاعات برای انجام فعالیت‌های هماهنگ راهبری رخدادهای فضای تبادل داده و توسعه امنیت فضای تبادل اطلاعات و ارتباطات در کشور است؛ عمده فعالیت‌های این مرکز بر روی شبکه‌های مبتنی بر آی‌پی و شبکه‌های اینترنتی متمرکزشده است (سایت اینترنتی تیم پاسخ‌گویی فوریتی مرکز ماهر[۵]).

---

۱- Unauthorized Acces.

۲ – Inappropriate Usage.

۳- complex attacks.

٤- Scarfone.

٥- WW.CER.IR.

مرکز ماهر، مرکز هماهنگ کننده واکنش به رخدادها در کشور است و زیر نظر وزارت فناوری اطلاعات به عنوان تیم پاسخ‌گویی هماهنگ‌کننده را در کشور داشته و عمده وظایف این مرکز به‌صورت زیر است:

- تبادل اطلاعات بین تیم‌های پاسخ‌گویی دستگاه‌های مختلف کشور
- مسئولیت هماهنگی بین گوهر[1] دستگاه‌های مختلف کشور، برای یک واکنش هماهنگ به یک رخداد رایانه‌ای در سطح کشور
- کمک فراگیر و همه‌جانبه در صورت وقوع رخدادهای رایانه‌ای عمومی
- آگاهی‌رسانی‌های مشترک از نقاط ضعف امنیتی و مشکلات شبکه‌های کشور

پیش‌گیری و مهار رخدادهای رایانه‌ای، مقوله‌ای بااهمیت در راستای توسعه امنیت فضای تبادل اطلاعات و ارتباطات کشور است، مرکز تحقیقات مخابرات ایران مراکز «آگاهی‌رسانی، پشتیبانی وامداد رخدادهای رایانه‌ای» که به‌اختصار «آپا» نامیده شده را بدین منظور ایجاد نموده است. تحقیقات این پروژه که در سطح ملی اجرا می‌شود به هشت دانشگاه اصلی کشور واگذارشده است. در حال حاضر هشت مرکز تخصصی آپا به ترتیب زیر ایجادشده‌اند که به‌مرور دامنه خدمات خود را پس از طی نمودن مراحل راه‌اندازی و تجهیز گسترش می‌دهند. مدیریت بخش‌های مختلف پرتال آپا به عهده گروه‌های آپا می‌باشد، که برخی از آن‌ها با حوزه ماموریتی به‌صورت زیر اشاره می‌شود:

- مرکز آپا در دانشگاه صنعتی شریف در حوزه رخدادهای مرتبط با بانک‌های اطلاعاتی؛
- مرکز آپا در دانشگاه صنعتی امیرکبیر در حوزه رخدادهای مرتبط با سیستم‌های عامل؛
- مرکز آپا در دانشگاه صنعتی اصفهان در حوزه رخدادهای مرتبط با تجهیزات شبکه؛
- مرکز آپا در دانشگاه امام حسین (ع) در حوزه رخدادهای مرتبط با سیستم‌های رمزنگاری؛
- مرکز آپا در دانشگاه یزد در حوزه رخدادهای مرتبط با نرم‌افزارهای کاربردی؛
- مرکز آپا در دانشگاه تربیت مدرس در حوزه رخدادهای مرتبط با اسپم؛
- مرکز آپا در دانشگاه فردوسی مشهد در حوزه رخدادهای مرتبط با سرویس‌های شبکه؛
- مرکز آپا در دانشگاه شیراز در حوزه رخدادهای مرتبط با بدافزار (سایت اینترنتی تیم پاسخ‌گویی فوریتی مرکز ماهر).

- مرکز ملی فضای مجازی که عمده شرح وظایف این مرکز به‌صورت زیر است:

جدول (۱): شرح وظایف مرکز ملی فضای مجازی (موارد احصاء شده از سند نظام ملی پیشگیری و مقابله با رخدادهای فضای مجازی)

| | |
|---|---|
| شرح وظایف مرکز ملی فضای مجازی | – پایش و رصد نظام‌مند و مستمر فرصت‌ها و تهدیدهای فضای مجازی برای کشور<br>– مدیریت تشخیص حملات سایبری به کشور هم‌چنین دفاع از زیرساخت‌های حیاتی در برابر حملات سایبری<br>– تشخیص حملات سایبری به کشور و هم‌چنین دفاع از زیرساخت‌های حیاتی در برابر حملات سایبری از داخل و خارج از کشور<br>– صیانت از زیرساخت‌های حیاتی در برابر حملات اینترنتی و دفاع مناسب در برابر هرگونه حمله<br>– پایش و رصد عالمانه، نظام‌مند و مستمر تهدیدات فضای مجازی برای کشور و تدابیر لازم برای مواجهه به‌موقع و مبتکرانه با آن‌ها |

۱- CSIRT.

| | |
|---|---|
| | – سامان‌دهی امنیت فضای مجازی کشور در شرایط عادی و بحرانی و همچنین تهیه و تصویب ضوابط، آیین‌نامه‌ها و دستورالعمل‌های موردنیاز در این عرصه<br>– مدیریت تشخیص حملات سایبری به کشور و هم‌چنین دفاع از زیرساخت‌های حیاتی در برابر حملات سایبری از داخل و خارج کشور |

پلیس فضای تولید و تبادل اطلاعات فراجا با نام مختصر پلیس فتا و مشهور به پلیس سایبری ایران، یک واحد تخصصی فرماندهی انتظامی جمهوری اسلامی ایران است که وظیفه آن جلوگیری و مبارزه با ایجاد فیشینگ (کلاهبرداری اینترنتی) و جعل، سرقت اینترنتی، هک، نفوذ و جرائم سازمان‌یافته رایانه‌ای است. (سایت اینترنتی پلیس فتا) و عمده شرح وظایف آن به‌صورت زیر است:

جدول (۲): شرح وظایف پلیس فتا (سایت اینترنتی پلیس فتا)

| | |
|---|---|
| شرح وظایف نیروی انتظامی (پلیس فتا) | – کوتاه نمودن دست اخاذان و تبهکاران از افراد (حقیقی و حقوقی)<br>– کاهش سرعت پاسخ‌گویی به رخدادهای رایانه‌ای و مقابله با آن<br>– مرجع امن سازی کسب‌وکارها در فضای مجازی (پلیس فتا)<br>– ارائه استانداردها، الزامات و مشاوره‌ها و همکاری در زمینه ارتقای سطح امنیت کسب‌وکارهای سالم اینترنتی<br>– تلاش همه‌جانبه برای همکاری و هم‌افزایی سازمان‌های مسوول و حفظ وفاق ملی در مواجهه با تهدیدات و مخاطرات فراگیر و عمیق سایبری کشور در همه حوزه‌ها |

## ۸- روش‌شناسی تحقیق

این تحقیق از حیث هدف تحقیقی، کاربردی است؛ از حیث سطح تحلیل، برخوردار از ماهیتی توصیفی– استنباطی و از حیث رویکرد و طبقه‌بندی روش، کتابخانه‌ای است. داده‌های موردنیاز از راه مطالعات کتابخانه‌ای و با استفاده از ابزار فیش‌برداری گردآوری شده است و با نظر خبرگان حوزه سایبری دفاعی، سوالاتی تنظیم شد و سپس سوالات در بین ٦٥ نفر از خبرگان که دارای شرایط و ویژگی‌های متناسب با موضوع پژوهش باشند، توزیع گردید و درنهایت نتایج آن از طریق نرم‌افزار اس‌پی‌اس‌اس، به‌عنوان نتایج تحقیق ارایه شده است.

این تحقیق کاربردی و توسعه‌ای است. نظر به وجود یک مدل مناسب برای پیاده‌سازی تیم پاسخ‌گویی فوریتی رایانه‌ای و با توجه به این‌که نتایج حاصل از پژوهش در حوزه دفاعی قابل بهره‌برداری است، در زمره تحقیقات کاربردی محسوب می‌شود؛ همچنین نظر به اهمیت تحقیق حاضر در پاسخ‌گویی به تهدیدات، این تحقیق قابلیت توسعه داشته و درنتیجه تحقیق حاضر توسعه‌ای می‌باشد.

روش تحقیق نیز آمیخته و ترکیبی از روش‌های توصیفی- تحلیلی و پیمایشی (مصاحبه و نخبگی) است.

جامعه آماری پژوهش حاضر شامل کلیه خبرگان، صاحب‌نظران و متولیان کشور و نیروهای مسلح جمهوری اسلامی ایران که واجد ویژگی‌های زیر بوده‌اند:

– دارا بودن حداقل مدرک تحصیلی کارشناسی ارشد

– دارا بودن جایگاه شغلی راهبردی فناوری اطلاعات

– صاحب‌نظر و مجرب در مباحث راهبردی فناوری اطلاعات

در بررسی مقدماتی و طی مشورت با چند تن از خبرگان، حجم جامعه آماری از ۲۰ نفر تشکیل‌شده است و با توجه به محدود بودن حجم جامعه آماری، نمونه آماری به جامعه آماری منطبق و روش نمونه‌گیری تمام شمار است.

نظر به این‌که محققین به دنبال تبیین راهکارهایی برای ایجاد امنیت و مقابله با تهدیدات رایانه‌ای بوده‌اند، پس از مطالعه مبانی تئوری، تحلیل اسناد مربوطه، مصاحبه عمیق و هدفمند با خبرگان و صاحب‌نظران حوزه دفاع سایبری و واکاوی پیشینه‌های موجود با تأکید بر چارچوب نظری تحقیق، مدل مفهومی اولیه‌ای پیشنهاد شد و سپس با استفاده از داده‌های گردآوری‌شده، پرسش‌نامه محقق ساخته‌ای تنظیم گردید، سپس در یک جمع خبرگی ده‌نفره به روایی و پایایی آن پرداخته شد.

ابزارهای اصلی گردآوری اطلاعات بدین شرح است که با توجه به روند پژوهش، پس از تعیین شاخص‌ها، پرسش‌نامه به ٦٥ نفر از صاحب‌نظران و خبرگان دفاعی– امنیتی در حوزه فناوری اطلاعات ارایه شد و درنهایت با روش توصیفی– آماری، تحلیل اسناد و مدارک و تحلیل سیستماتیک بر روی داده‌ها انجام شد.

## ۹- بررسی برخی از تیم‌های پاسخ‌گویی رایانه‌ای فعال در عرصه جهانی

امروزه کشورهای فراوانی موفق به راه‌اندازی تیم پاسخ‌گویی فوریتی رایانه‌ای شده‌اند و آن را در لایه‌های مختلف مدیریتی و زیرساختی به‌کارگیری نموده‌اند؛ در زیر به بررسی برخی از تیم‌های پاسخ‌گویی، در حوزه ملی و در حوزه دفاعی اشاره‌شده است:

### ۹-۱- تیم پاسخ‌گویی فوریتی رایانه‌ای ایالات‌متحده آمریکا[1]

کشور ایالات‌متحده آمریکا در زمینه امنیت اطلاعات و ارتباطات، پیشرفته‌ترین کشور محسوب می‌شود و دارای ساختارهای فراوان و پیچیده‌ای در زمینه اطلاعات و ارتباطات است. این ساختارها به ویژه بعد از حادثه ۱۱ سپتامبر سال ۲۰۰۱، موردبازنگری جدی و اساسی قرار گرفت و با ایجاد وزارتخانه جدیدی به نام «وزارت امنیت داخلی»، مسئولیت‌های مرتبط با امنیت و خصوصاً امنیت فضای سایبر، به‌طورکلی زیر نظر این وزارتخانه قرار گرفت.

در راهبرد امن سازی فضای سایبر آمریکا سه هدف نهایی زیر تعیین‌شده‌اند:

۱- جلوگیری از حملات علیه زیرساخت‌های اطلاعاتی حیاتی کشور،

۲-کاهش نفوذپذیری‌ها،

۳-به حداقل رساندن خسارات و زمان احیاء.

ایالات‌متحده آمریکا به‌عنوان پیش‌گام در این موضوع، اولین تیم پاسخ‌گویی را در سال ۱۹۸۹ در دانشگاه کارنگی ملون ایجاد نمود و همچنین برای راه‌اندازی تیم پاسخ‌گویی و منابع آموزشی، سایت اینترنتی مرجع تیم‌های پاسخ‌گویی فوریتی رایانه‌ای[2] را ایجاد نمود که بهترین مرجع اینترنتی در این حوزه می‌باشد (رشتی، ۱۳۸۸: ۱۲-۸).

---

۱- US-CERT.

۲- www.CERT.org.

### ۹-۲- تیم پاسخ‌گویی فوریتی رایانه‌ای گارد ساحلی ایالات‌متحده آمریکا[۱]

تیم پاسخ‌گویی گارد ساحلی اولین عنصر از ساختار عملیاتی دفاعی شبکه رایانه‌ای است. کارهایی که در دفاع از سیستم‌های اطلاعاتی گارد ساحلی انجام می‌شود، نیاز به هماهنگی نزدیک با وزارت دفاع و وزارت میهن دارد و این‌یکی از وظایف عمده این تیم است. برنامه سایبری گارد ساحلی برای بهبود امنیت و دفاع شبکه گارد ساحلی تعیین‌شده است. افسر ارشد اطلاعات گارد ساحلی به‌عنوان مدیر فعالیت می‌کند و به دستیار فرمانده اطلاعات و تحقیقات جنایی گزارش می‌دهد. هدف اصلی برنامه تیم پاسخ‌گویی گارد ساحلی، دفاع از شبکه‌ها، سیستم‌های اطلاعاتی و داده‌های گارد ساحلی است. پاسخ‌گویی به رخدادهای رایانه‌ای گارد ساحلی، عنصر اصلی عملیاتی دفاع شبکه رایانه‌ای است. کارهایی که در دفاع از سیستم‌های اطلاعاتی گارد ساحلی انجام می‌شود، نیاز به هماهنگی نزدیک با وزارت دفاع و وزارت امنیت داخلی برای ارائه نشانه‌ها و هشدارهای تهدیدات سایبری در حوزه دریایی دارد. اگرچه هدف اصلی برنامه سایبری گارد ساحلی، دفاع از شبکه‌های گارد ساحلی است، اما برنامه سایبری گارد ساحلی همچنین با امنیت داخلی[۲]، سایر ارگان‌های دولتی و صنعت در حال تعیین بحث برای تعیین نقش‌ها و مسئولیت‌های شناسایی و کاهش خطرات سایبری در سیستم حمل‌ونقل دریایی بوده است (سالی برایس و اوهارا[۳]، ۲۰۱۷: ٦).

### ۹-۳- تیم پاسخ‌گویی فوریتی رایانه‌ای ارتش آمریکا[٤]

انجمن دفاع رایانه‌ای ارتش آمریکا که برای اطمینان از امنیت کلی، توسط تیم واکنش فوریتی رایانه ارتش آمریکا ایجاد شده است و شامل سه نوع مأموریت زیر است:

۱. بازدید دوره‌ای از شبکه: نقاط ضعف امنیتی شبکه رایانه‌ای را شناسایی و اصلاح می‌نماید.

۲. تحلیل آسیب شبکه: اقدامات متقابل را شناسایی، اصلاح و توصیه می‌کند.

۳. تست نفوذ مداوم: از شبکه‌های فعال، به‌صورت مداوم تست نفوذ و ارزیابی دوره‌ای انجام می‌نماید (نشریه فعالیت‌های سایبری مرکز تحقیقات دفاعی ایالات‌متحده[۵]، ۲۰۱۷: ۷۵).

### ۹-٤- تیم پاسخ‌گویی فوریتی رایانه‌ای وزارت دفاع هلند[٦]

تیم پاسخ‌گویی فوریتی رایانه‌ای وزارت دفاع هلند تیمی است که از تداوم عملیات و قابلیت اطمینان سیستم‌های اطلاعاتی مورداستفاده در نیروهای مسلح هلند پشتیبانی می‌کند. تیم پاسخ‌گویی این کار را با شناسایی و تجزیه وتحلیل تهدیدات سایبری و به دنبال آن کاهش و یا حذف هماهنگ تهدیدات انجام می‌دهد. همچنین می‌توان این تیم را برای حمایت از مباحث حقوقی سایبری تعیین کرد (سایت اینترنتی ایتلاو[۷]).

---

۱- Coast Guard Computer Incident Response Team(CGCIRT).

۲- DHS.

۳- Sally Brice-O Hara.

٤- U.S. Army Computer Emergency Response Team (ACERT).

۵- DOD Faces Challenges In Its Cyber Activities.

٦- The Computer Emergency Response Team of the Ministry of Defence (DefCERT).

۷- itlaw.wikia.org.

### ۹-۵- تیم پاسخ‌گویی فوریتی رایانه‌ای فنلاند

در سال ۲۰۰۱ میلادی تشکیلاتی تحت عنوان «کمیته مشورتی امنیت اطلاعات» زیر نظر ریاست جمهوری در فنلاند ایجاد شد. هدف اولیه از تشکیل این کمیته، ارتقاء امنیت فضای سایبر کشور در سطح مردم، شرکت‌ها، سازمان‌ها و دولت‌ها تعیین گردید. در سال ۲۰۰۲، این کمیته مسئولیت ارائه راهبرد ملی امنیت فضای سایبر کشور فنلاند و همچنین نظارت بر پیاده‌سازی راهبرد تصویب‌شده را بر عهده گرفت. با توجه به اهمیت این نگرش بلندمدت در این زمینه، در ماه مه سال ۲۰۰۲ تیم پاسخ‌گویی فوریتی رایانه‌ای فنلاند تشکیل شد؛ خط‌مشی‌های منتج از چشم‌انداز تیم پاسخ‌گویی در فنلاند عبارت‌اند از:

-همکاری و تعامل بین‌المللی؛

-تقویت و هماهنگ‌سازی نقش‌های مختلف فعال درصحنه؛

- مدیریت و پشتیبانی توسعه امنیت فضای تبادل اطلاعات کشور در سطح ملی؛

حمایت از توسعه و سربلندی جامعه از طریق بهبود امنیت اطلاعات با اهداف زیر:

- ارتقاء و حمایت از ایجاد روال‌ها، محصولات، خدمات و ساختارهای امن؛

- پشتیبانی از قابلیت دسترس و قابل‌استفاده بودن اطلاعات؛

- تقویت مدیریت مخاطرات امنیت اطلاعات؛

- حفاظت از زیرساخت‌ها؛

- حفاظت از حقوق اساسی افراد (بروان لی، ۲۰۱۸: ۱۹).

### ۱۰- فرآیند، مدل‌ها و خدمات مهم تیم پاسخ‌گویی فوریت‌های رایانه‌ای

در این بخش به مدل‌ها، خدمات، جایگاه سازمانی، میزان اختیار و دیگر مولفه‌های تاثیرگذار تیم پاسخ‌گویی پرداخته‌شده است؛ قبل از لازم به ذکر است که فرآیند پاسخ‌گویی به رخدادهای رایانه‌ای به شرح زیر است:

روش پاسخ‌گویی به رخداد مطابق شکل (۱) دارای چندین بخش می‌باشد. هریک از این بخش‌ها در یک چرخه تحت عنوان چرخه حیات پشتیبانی حوادث از جایگاه مشخصی برخوردار می‌باشند.

### ۱۰-۱- فرآیند پاسخ‌گویی به رخداد از دید اتحادیه بین‌المللی استاندارد و فناوری[۱]

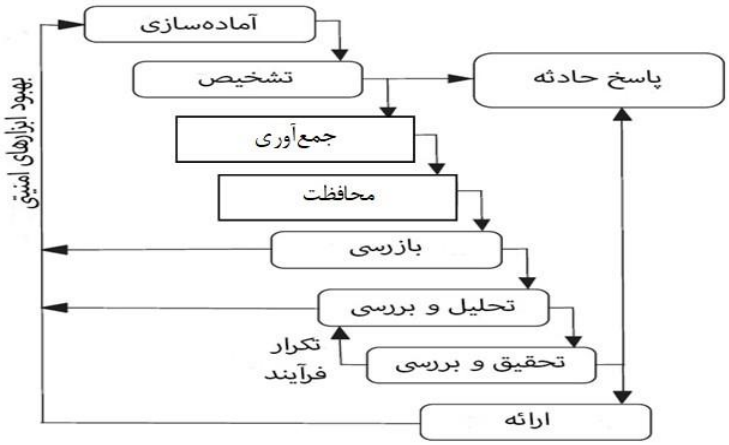
یک فرآیند در پاسخ‌گویی به رخداد، قسمتی از یک چارچوب مدیریتی ارتباطی خوب است که با داشتن یک روش مناسب، اقدام به پاسخ‌گویی به رخداد می‌نماید. مهم‌ترین این روش‌ها در چارچوب پاسخ‌گویی به رخدادهایی توسط متخصصان دانشگاه دیپوال[۲] با تیم مهندسی نرم‌افزار انستیتو کارنگی‌ملون و انستیتو استاندارد و فناوری طراحی نموده‌اند که هدف از آن کوتاه‌تر کردن دامنه اثرات رخدادها می‌باشد. بااین‌حال استاندارد خاصی جهت گسترده کردن وجود ندارد. به‌منظور این‌که در زمان وقوع یک رخداد یک طرح پویا و موثری داشته باشیم از طرحی مشابه شکل (۱) استفاده می‌کنیم که بر اساس طرح انستیتو استاندارد و فناوری[۳] عمل می‌نماییم. ما خودمان را به اقداماتی که در هر فاز

۱- National Institute of Standards and Technology(NIST).

۲- Depaul.

۳- NIST.

می‌بایستی انجام بدهیم محدود می‌کنیم بدون این‌که از همه اختیارات ممکن و راه حل‌های نسبی خارج شویم (علیدوستی، ۱۳۹۲: ۸۲)




شکل (۱): مراحل آماده‌سازی در مراحل وقوع رخداد از دید انستیتو استاندارد و فناوری (علیدوستی، ۱۳۹۲)

مدل ارائه‌شده قابل کاربرد به‌صورت بی‌درنگ و پس از حمله می‌باشد. پنج مرحله اول بر ترافیک بی‌درنگ شبکه عمل می‌کنند. مرحله آماده‌سازی تضمین می‌کند که تجهیزات نظارتی در جایگاه خود قرار دارند. مرحله تشخیص در کشف حمله کمک می‌کند و مرحله جمع‌آوری، بسته‌های شبکه را گرفته و صحت داده‌ها را تضمین می‌کند. پاسخ مناسبی به رخداد بر اساس ماهیت حمله تولید می‌شود و در مرحله محافظت، درهم‌سازی داده‌ها ایجاد شده و یک کپی از آن ساخته می‌شود. چهار مرحله بعد برای سناریوهای بی‌درنگ و پس از حمله کاربرد دارند. رسیدگی پس از حمله از مرحله آزمایش شروع می‌شود، جایی که یک کپی از فایل دریافت بسته مرحله آزمایش ورودی منابع مختلف را ترکیب می‌کند و شاخص‌های حمله را شناسایی می‌کند. مرحله تحلیل با روش‌های استخراج داده، محاسبات نرم و آماری الگوهای حمله را طبقه‌بندی می‌کند. مرحله بازرسی شامل ردیابی و شناسایی مهاجم می‌باشد. مرحله نهایی ارائه منجر به تعقیب قانونی مهاجم می‌شود (همان: ۸۳).

### ۱۰-۲- فرآیند پاسخ‌گویی به یک رخداد رایانه‌ای

در فرآیند پاسخ‌گویی، باید به دسته‌بندی و نحوه اولویت‌بندی و سپس ارسال گزارش به بخش‌های پاسخ‌گویی توجه داشت؛ پس از دریافت گزارشات از طریق تلفن، ایمیل، تجهیزات هشداردهنده و غیره، این گزارشات باید از طریق تریاژ به واحدهای پاسخ‌گو ارسال شوند.

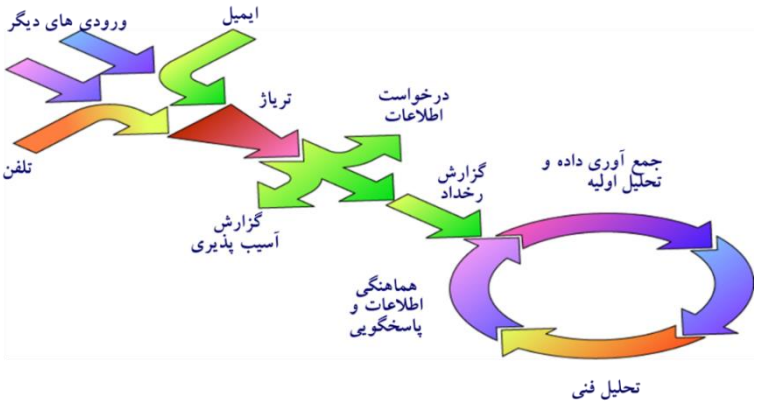
گزارش‌گیری (تریاژ)، فرآیند دسته‌بندی، رده‌بندی و اولویت‌بندی گزارش‌های رخداد یا سایر درخواست‌ها به تیم پاسخ‌گویی است این امر را می‌توان با تریاژ بیمارستان‌ها مقایسه نمود، جایی که بیماران اورژانسی از سایر بیماران تفکیک می‌شوند.

تریاژ یک عنصر اساسی هر تیم پاسخ‌گویی است و برای درک آن چه در سازمان گزارش داده می‌شود ضروری است؛ تریاژ نگاهی اجمالی به فعالیت‌های در حال انجام به تیم پاسخ‌گویی می‌دهد. این فرآیند می‌تواند به شناسایی مشکلات بالقوه امنیتی و اولویت‌بندی گزارشات ارسالی به تیم پاسخ‌گویی کمک کند (اسکارفن و همکاران[۱]، ۲۰۱۸: ۱۴۰).

۱- Scarfone.

تیم پاسخ‌گویی خط تلفن یا میز امداد اختصاصی خود را در سازمان دارد که کارکنان آن از اعضای تیم هستند. این کارکنان تمامی گزارش‌ها و درخواست‌هایی را که توسط تلفن، پست الکترونیکی و وب دریافت می‌شود، طبقه‌بندی و اولویت‌بندی می‌کنند. سپس گزارش‌های مربوط به آسیب‌پذیری یا رخداد امنیتی برای بررسی به تحلیل‌گران مربوطه در تیم پاسخ‌گویی ارجاع داده می‌شود (همان: ۱٤۱).

با توجه به تعریف تریاژ، فرآیند نحوه پاسخ‌گویی به یک رخداد رایانه‌ای در شکل (۲) ترسیم‌شده است؛ ورودی‌ها شامل ایمیل، اخبار و اطلاعات، تلفن، تیکت و غیره است که پس از ورود به بخش تریاژ، دسته‌بندی و اولویت‌بندی شده و درصورتی‌که با توجه به علائم موجود و گزارش‌های قبلی، به‌عنوان رخداد شناخته شود، گزارش رخداد به تیم فنی رفته و پس از جمع‌آوری اطلاعات و تحلیل اولیه، به آن رخداد پاسخ داده خواهد شد.




شکل (۲): نمونه‌ای از فرآیند پاسخ‌گویی به یک رخداد رایانه‌ای (Scarfone, et.al, ۲۰۱۸)

در تحلیل، تیم فنی متشکل از معاونین و کارشناسان فنی شبکه، به تحلیل آن پرداخته و اگر راهکار آن توسط کارشناسان داخلی وجود داشته باشد اقدام به پاسخ‌گویی نموده و در غیر این صورت برای مراکز پاسخ‌گویی خارجی (مانند مرکز ماهر) ارسال می‌شود و مرکز پاسخ‌گویی خارجی اقدام به پاسخ‌گویی و برطرف نمودن آن رخداد خواهد نمود؛ یکی از اقدامات مهم دیگر تیم مباحث جرم‌شناسی است که پس از گرفتن آدرس مهاجمان و لاگ‌های دریافتی و دیگر اسناد مهم، برای مباحث قانونی اقدام می‌نمایند.

مولفه‌های تنظیم مقررات و حقوقی شامل موارد زیر است: دسترسی به مشاوره حقوقی: تجزیه وتحلیل قرارداد، تعریف خدمات و تضمین کیفیت، سیاست‌ها و رویه‌ها (مارتین وندرهای[۱]، ۲۰۱۷: ۹) و دریافت مجوز از مدیریت ارشد، استانداردها، پیگیری یا ردیابی (جان فرانکو دبت[۲]، ۲۰۱۷: ٦).

### ۱۰-۳- جدول محاسبات ارزیابی ریسک و مخاطرات

یکی از بخش‌هایی که در اولویت‌بندی تیم پاسخ‌گویی مراکز دفاعی مطرح می‌گردد ارزیابی ریسک و مخاطرات است؛ در جدول ۳، ارزیابی تهدیدات و مخاطرات را در مراکز دفاعی می‌توان به‌صورت زیر محاسبه نمود و پس از تقاطع گیری، مشخص خواهد شد که اگر در جداول با خانه‌های ۰،۱ و ۲ باشد همه‌چیز تحت کنترل است؛ خانه‌های

۱- Martijn van der heide.

۲- John Franco Dept.

۳، ٤ و ٥ تهدید سایبری است و ٦ و ۷ بحران سایبری و عدد ۸ بیانگر جنگ سایبری در مراکز دفاعی است؛ اما به لحاظ اینکه قلمرو این مقاله فقط شبکه‌های رایانه‌ای است، حوزه کاری را فقط به شبکه رایانه‌ای محدود می‌کنیم (سازمان پدافند غیرعامل کشور، ۱۳۹۳: ٤۱). در این طرح پس از وقوع هر یک از پیشامدهای ممکن، راهکارها و مراجع مختلف برای پاسخ‌گویی اقدام خواهند نمود و در بخش بعد فرآیندی را که تیم پاسخ‌گویی رایانه‌ای مراکز امنیتی باید انجام دهند تشریح گردیده است.

جدول ۳- جدول ارزیابی ریسک و مخاطرات مراکز دفاعی

| احتمال وقوع / شدت پیامد | خیلی غیرمحتمل | غیرمحتمل | ممکن | محتمل | قریب‌الوقوع |
|---|---|---|---|---|---|
| خیلی کم (تحت کنترل) | ۰ | ۱ | ۲ | ۳ | ۴ |
| کم (حادثه‌آفرین) | ۱ | ۲ | ۳ | ۴ | ۵ |
| متوسط (مخل امنیت) | ۲ | ۳ | ۴ | ۵ | ۶ |
| زیاد (بحران‌زا) | ۳ | ۳ | ۵ | ۶ | ۷ |
| خیلی زیاد (فاجعه‌بار) | ۴ | ۵ | ۶ | ۷ | ۸ |

وضعیت سفید = تحت کنترل سایبری= ۰،۱،۲

وضعیت زرد = تهدید سایبری= ۳،۴،۵

وضعیت نارنجی = بحران سایبری= ۶،۷

وضعیت قرمز = جنگ سایبری= ۸

## ۱۰-٤- مدل‌های به‌کارگیری تیم پاسخ‌گویی

### الف- گروه امنیتی (به‌کارگیری کارکنان موجود فن‌آوری اطلاعات)

این مدل، یک تیم پاسخ‌گویی رسمی نیست. فعالیت‌های پاسخ‌گویی به حادثه توسط مدیران امنیتی، شبکه و سیستم که مسئول نگهداری و پیکربندی شبکه‌ها و رایانه‌های سازمان هستند در همان نقطه حل‌وفصل می‌گردد. از مدیران سیستم، شبکه و امنیت که این کار را انجام می‌دهند، به‌عنوان «گروه امنیتی» نام‌برده می‌شود. مشکلی این مدل نبود راهی برای تضمین پاسخ‌گویی صحیح و منسجم در کل سازمان است (کیلکرس[۱] و همکاران، ۲۰۱٦: ۷۵-۷۳).

### ب- تیم پاسخ‌گویی توزیع‌شده داخلی

در چنین الگویی که تیم پاسخ‌گویی «پراکنده» نیز نامیده می‌شود، گروه ترکیبی از کارکنانی به مدیریت مرکزی تیم پاسخ‌گویی گزارش می‌دهند. این گروه به این علت «داخلی» خوانده می‌شود که گروهی در داخل یک سازمان است. این گروه به دلایل: ۱) وجود فرآیندها، روش‌ها و سیاست‌های رسمی‌تر در حل‌وفصل حادثه‌ها،

۱- Killcrece.

۲) ایجاد روش ارتباطی با کل تشکیلات درباره تهدیدات امنیتی و راهبرد پاسخ‌گویی و ۳) اعضای گروه و یک مدیر تیم پاسخ‌گویی معین که به صورت اختصاصی برای وظایف رفع یک حادثه تعیین شده‌اند از الگوی گروه امنیتی متفاوت است (آلبرت، دروفی، کیلکرس، رافائل[۱]، ۲۰۱٦: ۲٤).

## ج- تیم پاسخ‌گویی متمرکز داخلی

مدل تیم پاسخ‌گویی متمرکز داخلی، یک تیم پاسخ‌گویی اختصاصی است که در سازمان متمرکز شده است و مسئولیت کامل گزارش دهی، تحلیل و پاسخ‌گویی به همه حادثه‌ها را بر عهده دارد. در این حالت معمولاً اعضای تیم کل وقت خود را به کارهای مربوط به تیم پاسخ‌گویی و رفع حادثه‌ها اختصاص می‌دهند. این نوع تیم پاسخ‌گویی دارای مدیری است که به مدیریت رده‌بالای سازمان گزارش می‌دهد. تمامی منابع تیم پاسخ‌گویی در یک نقطه متمرکز شده‌اند. این مدل در با نام «تیم پاسخ‌گویی متمرکز» نیز شناخته می‌شود (همان: ۲۵).

## د- تیم پاسخ‌گویی ترکیبی (توزیع‌شده و متمرکز یا هیبریدی)

در این مدل، یک تیم پاسخ‌گویی متمرکز اختصاصی به وجود می‌آید که اعضای آن در سازمان، در موقعیت‌های جغرافیایی و شعب مختلف توزیع‌شده‌اند. این تیم مرکزی کار تحلیل را در سطح بالا انجام می‌دهد و راهبردهای بازیابی از حادثه‌ها و رفع آن‌ها را تدوین می‌کند. همچنین کار پشتیبانی پاسخ‌گویی به حادثه‌ها، آسیب‌پذیری‌ها و بسته‌های مشکوک[۲] را برای اعضای توزیع شده تیم و سایر بخش‌های سازمان انجام می‌دهد. اعضای پراکنده تیم در هر سایت راهبردها را پیاده‌سازی می‌کنند و در حوزه‌های مسئولیت خود، مهارت و دانش خود را در اختیار دیگران قرار می‌دهند. این مدل با عنوان تیم پاسخ‌گویی ترکیبی شناخته می‌شود (همان: ۳۳).

نقاط قوت و ضعف هر یک از مدل‌ها به تفکیک در جدول (٤) آمده است

جدول ۴: نقاط قوت و ضعف مدل تیم‌های پاسخ‌گویی (کاساکواساکی[۳] و همکاران، ۲۰۱۷)

| ردیف | گروه امنیتی | توزیع‌شده داخلی | متمرکز داخلی | توزیع‌شده و متمرکز | هماهنگ‌کننده |
|---|---|---|---|---|---|
| نقاط قوت | - هیچ نقطه قوتی به دلیل نبود حل‌وفصلی مشاهده نمی‌شود. | - تمرکز در مسئولیت - یکپارچگی در ماموریت<br>- داشتن پایگاه داده متمرکز<br>- داشتن دیدگاه جامع<br>- قابلیت نیروهای محلی | - داشتن کارکنان متمرکز و اختصاصی و آموزش‌دیده<br>- شناسایی حمله‌های هدف‌دار<br>- داشتن پایگاه داده قوی<br>- پشتیبانی آموزشی قوی رده‌ها<br>- سهولت در حفظ تیم | - داشتن نیروهای متمرکز و توزیع‌شده<br>- داشتن پایگاه قوی داده<br>- یکپارچگی در ماموریت<br>- مسئولیت متمرکز و تلفیقی<br>- پشتیبانی آموزشی قوی رده‌ها<br>- سهولت در پیاده‌سازی دستورالعمل‌ها | - دارای کارکنان اختصاصی و کارآزموده<br>- دارای یک واحد قوی گزارش دهی<br>- دارای واحدی متمرکز برای تحلیل اطلاعات<br>- دارای یک پایگاه داده قوی<br>- وجود تریاژ در خارج از سازمان<br>- پشتیبانی قوی آموزشی رده‌ها |
| نقاط ضعف[۱] | | | | | |

۱- Albert,C, Dorofee,A,Killcrece, G, Ruefle,.

۲- Artifacts.

۳- Kossakowski.

### ۵- تیم پاسخ‌گویی هماهنگ‌کننده

در این مدل تمرکز اصلی تیم پاسخ‌گویی هماهنگ نمودن و تسهیل فعالیت‌های رسیدگی به حادثه و آسیب‌پذیری در یک سطح گسترده، پراکنده و معمولاً مراکز تحت پوشش خارجی است. این هماهنگی و تسهیل می‌تواند شامل به اشتراک گذاشتن اطلاعات، ارائه راهبردها و توصیه‌های کاهش زیان برای بازیابی و پاسخ‌گویی به حادثه، تحلیل و پژوهش در مورد روندها و الگوهای فعالیت حادثه‌ها در مراکز تحت پوشش، ارائه منابع و مراجع برای مدیریت حادثه نظیر پایگاه‌های داده آسیب‌پذیری، بنگاه‌های پایاپای سازی ابزارهای امنیتی، یا خدمات اعلان خطر و مشاوره باشد (آلبرت، دروفی، کیلکرس، رافائل، ۲۰۱۶: ۱۷۵).

### ۱۰-۵- اختیار[۲]

اختیار به معنی میزان تسلط تیم پاسخ‌گویی بر فعالیت‌های مرتبط با امنیت رایانه و رفع حادثه امنیتی مراکز تحت پوشش است. اختیار، نوع ارتباط تیم پاسخ‌گویی را با مشتریان نشان می‌دهد. تیم پاسخ‌گویی با سه سطح متفاوت اقتدار در مراکز تحت پوشش آن وجود دارد: اقتدار کامل، اشتراکی و فقدان اقتدار.

#### ۱۰-۵-۱- اختیار کامل

یعنی این‌که تیم پاسخ‌گویی قادر است مراکز تحت پوشش خود را مجبور کند اقدامات لازم را جهت ارتقاء وضعیت امنیتی سازمان یا بازیابی از یک حادثه انجام دهند. در این حالت، هنگامی‌که یک حادثه امنیتی اتفاق می‌افتد تیم پاسخ‌گویی می‌تواند در صورت لزوم، بدون آنکه منتظر اجازه مدیران رده‌بالا بماند تصمیم‌گیری کند. برای مثال یک تیم پاسخ‌گویی، بااقتدار کامل می‌تواند در صورت بروز یک حمله، به مدیران سیستم‌ها اعلام کند تا آن‌ها را از شبکه قطع کنند (سایت اینترنتی مرجع تیم پاسخ‌گویی فوریتی رایانه‌ای[۳]،۲۰۱۷).

#### ۱۰-۵-۲- اختیار مشارکتی

یعنی این‌که تیم پاسخ‌گویی می‌تواند در فرآیند تصمیم‌گیری در خصوص اقدامات لازم برای مراکز تحت پوشش مشارکت نماید. در این حالت تیم پاسخ‌گویی قادر است بر نتیجه تصمیم‌گیری تأثیر بگذارد اما تنها بخشی از فرآیند تصمیم‌گیری است و نه تصمیم‌گیرنده. در چنین شرایطی تیم پاسخ‌گویی می‌تواند به مدیران شبکه توصیه کند که هنگام بروز حمله، از شبکه قطع شوند و اقدامات لازم (با توجه به توصیه‌های ارائه‌شده) را با سایر اعضای مراکز تحت پوشش در میان بگذارند (کاساکواساکی و همکاران، ۲۰۱۷: ۳۶).

#### ۱۰-۵-۳- فقدان اختیار

یعنی این که تیم پاسخ‌گویی تنها می‌تواند به‌عنوان یک مشاور (البته بسیار قوی) برای یک سازمان عمل کند. این تیم نمی‌تواند به‌تنهایی هیچ تصمیمی بگیرد یا اقدامی انجام دهد. این تیم می‌تواند توصیه کند که سیستم‌ها هنگام بروز

---

۱- جهت اطلاع بیشتر ر.ک. به دفتر فصلنامه.

۲- Authority.

۳- CERT.org/ CSIRTServices.

حمله قطع شوند اما هیچ‌گونه تأثیری در تصمیم‌گیری نهایی نخواهد داشت. بااین‌حال می‌توان در صورت عدم تبعیت مراکز از توصیه‌های تیم پاسخ‌گویی اختیار افزایش اقدامات امنیتی را برای این تیم در نظر گرفت. در این حالت ممکن است به دلیل موقعیت و جایگاه خود در سازمان، بتواند بر تصمیم‌گیرندگان تیم پاسخ‌گویی تأثیر مثبتی داشته باشد (همان: ۳۷).

### ۱۰-٦- انواع خدمات قابل‌ارائه تیم پاسخ‌گویی

در حقیقت استانداردی از مجموعه کارها و سرویس‌هایی که یک تیم پاسخ‌گویی به حوادث رایانه‌ی باید ارائه دهد وجود ندارد و هر تیمی باید سرویس‌های خود را بر اساس نیازهای سازمان تعیین کند. ولی سرویس‌هایی که عموماً توسط تیم پاسخ‌گویی به حوادث رایانه‌ای ارائه می‌شود را می‌توان در سه گروه رده‌بندی کرد: سرویس‌های واکنشی، سرویس‌های پیش‌گیرانه و سرویس‌های مدیریت کیفیت امنیت (کیلکرس و همکاران، ۲۰۱٦: ۷۳).

### الف: خدمات انفعالی (واکنشی)

ارائه این خدمات، از طریق یک حادثه یا درخواست آغاز می‌شود. مانند گزارشی از به خطر افتادن یک میزبان، کدهایی که با سوء نیت و در حد وسیع منتشرشده‌اند، آسیب‌پذیری رایانه‌ای یا موردی که توسط کشف یک سیستم ردیابی اختلال یا ثبت ورود شناسایی‌شده است، خدمات واکنشی وظایف پایه‌یک تیم پاسخ‌گویی هستند (کاساکواساکی و همکاران، ۲۰۱۷: ۷٤).

### ب: خدمات غیرانفعالی (پیش‌گیرانه)

این خدمات، راهنمایی‌ها و اطلاعات لازم برای کمک به آماده‌سازی، حفاظت و ایمن‌سازی سیستم‌های تحت پوشش را فراهم می‌کنند. ارائه چنین خدماتی، به کاهش تعداد حوادث آتی می‌انجامد (کیلکرس و همکاران، ۲۰۱٦: ۷٤).

### ج: خدمات مدیریت کیفیت امنیت

این خدمات موجب تکمیل خدمات از قبل تعیین‌شده است که مستقل از رسیدگی به حوادث هستند و به‌صورت سنتی توسط دیگر بخش‌های سازمان همانند بخش‌های فناوری اطلاعات، بازرسی، یا آموزشی ارائه می‌شوند (همان: ۷٦). این خدمات در جدول (۵) فهرست شده است.

جدول (۵): خدمات مدیریت کیفیت امنیت (کیلکرس و همکاران، ۲۰۱۶).

| خدمات انفعالی (واکنشی) | خدمات غیرانفعالی (پیش‌گیرانه) | خدمات مدیریت کیفیت امنیت |
|---|---|---|
| اخطارها و اعلام خطرها | اطلاع‌رسانی | تحلیل ریسک |
| رسیدگی به حادثه | نظارت بر فناوری | برنامه‌ریزی تداوم کسب‌وکار |
| تحلیل حادثه | ممیزی یا ارزیابی امنیتی | مشاوره امنیتی |
| پاسخ‌گویی به حادثه در محل | پیکربندی و نگهداری ابزارها، برنامه‌ها و زیرساخت‌های امنیتی | آگاه‌سازی |
| پشتیبانی از پاسخ‌گویی به حادثه | توسعه ابزارهای امنیتی | تربیت/آموزش |

| | | |
|---|---|---|
| هماهنگی پاسخ‌گویی به حادثه | خدمات ردیابی اختلال | ارزیابی یا صدور گواهی برای محصول |
| بررسی، رسیدگی و پاسخ‌گویی به آسیب‌پذیری | انتشار اطلاعات امنیتی | بازیابی از فجایع |
| بررسی و تحلیل بسته‌های مشکوک | | |

باید توجه کرد که برخی خدمات هم بعد پیش‌گیرانه و هم بعد واکنشی دارند. برای مثال رسیدگی به آسیب‌پذیری می‌تواند در واکنش و پاسخ به کشف آسیب‌پذیری در نرم‌افزار صورت گیرد اما این امر به‌صورت پیش‌گیرانه نیز می‌تواند صورت پذیرد که با بررسی و آزمایش کدها برای تعیین محل آسیب‌پذیری‌ها قابل انجام است، بدین ترتیب مشکلات قبل از اینکه به‌طور وسیع خود را نشان دهند یا مورد بهره‌برداری قرار گیرند، قابل‌حل خواهند بود (همان: ۷۷). در ادامه ساختار تیم پاسخ‌گویی موردنیاز مراکز دفاعی که شامل مأموریت‌ها، اهداف و مقاصد، محدوده عملکرد، نوع و سطح سرویس‌ها، میزان اختیارات تیم، جایگاه آن در سازمان، مدل‌سازمانی تیم پاسخ‌گویی ارایه می‌شود. در این روش راهکارها بر مبنای مطالعات صورت گرفته و استفاده از نظرات خبرگان و در قالب پرسش‌نامه انجام و مبنای تحقیق قرارگرفته است. در طرح کلان اولیه نوع مدل‌سازمانی، نیروی انسانی، اقتدار تیم پاسخ‌گویی، سازمان‌های سرویس‌گیرنده و سرویس‌های موردنیاز تیم پاسخ‌گویی مراکز دفاعی مشخص‌شده‌اند.

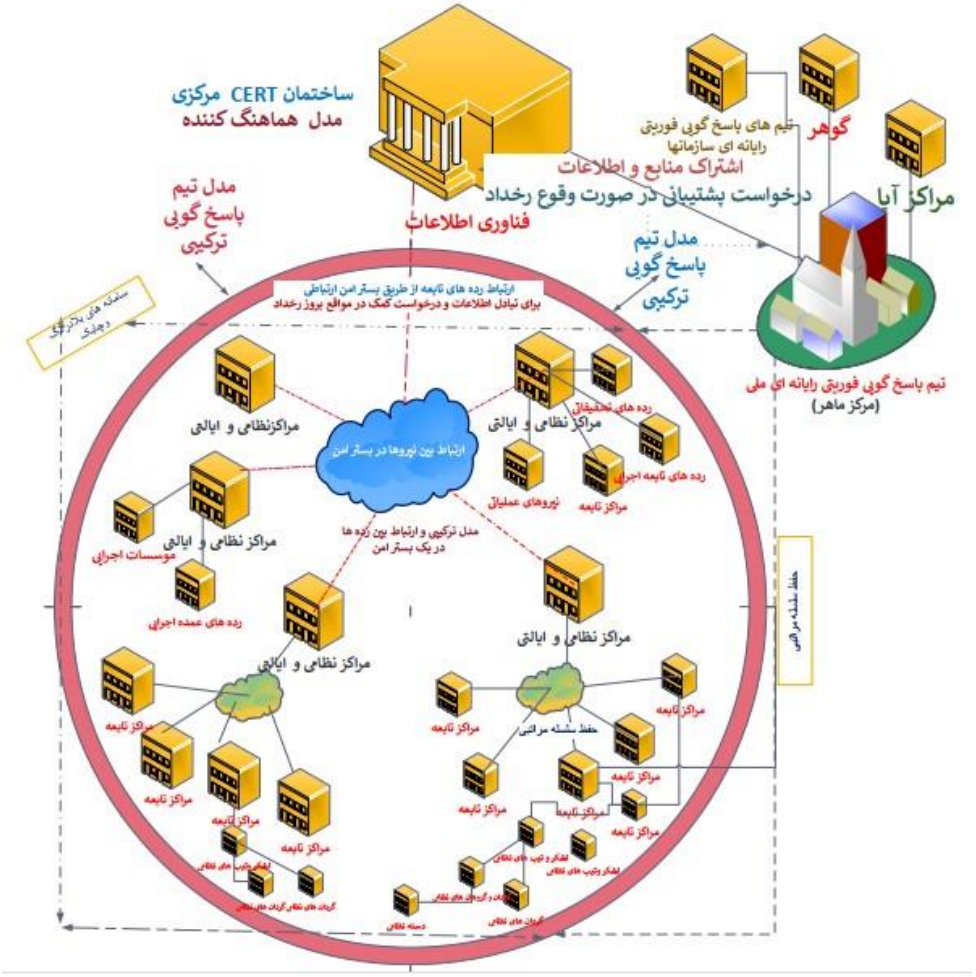
## ۱۱- تجزیه‌وتحلیل نتایج صورت گرفته (پیشنهاد مدل‌سازمانی، چارت سازمانی، بخش‌ها و سرویس‌های قابل ارایه تیم پاسخ‌گویی مراکز دفاعی)

پس از نظرسنجی از خبرگان دفاعی در حوزه سایبری و تنظیم پرسش‌نامه‌ها و تحلیل نتایج آماری، مدل‌سازمانی، چارت سازمانی و سرویس‌های تیم پاسخ‌گویی مراکز دفاعی به‌صورت زیر پیشنهاد می‌گردد:

### ۱۱-۱- مدل پیشنهادی سازمانی تیم پاسخ‌گویی فوریت رایانه‌ای

مدل‌سازمانی که باید برای مراکز دفاعی در نظر گرفته شود با توجه به محدوده جغرافیایی و پراکندگی سازمان و قرار گرفتن سرویس‌گرها و تجهیزات فناوری اطلاعات لحاظ می‌شوند. مراکز دفاعی با توجه به این‌که معمولا از گستردگی و پراکندگی بسیار بالایی برخوردار هستند و معمولا توان آن‌ها به صورت متمرکز در برخی از مراکز فرماندهی مستقر است، به‌صورت مرکزی مدیریت می‌شوند؛ ازاین‌رو در مدل پیشنهادی که با نظر خبرگان سایبری دفاعی تهیه گردید مدل ترکیبی (توزیع‌شده و متمرکز یا هیبریدی) برای همه رده‌های تابعه پیشنهاد گردید و ازآنجایی که امکان دسترسی هر مرکز دفاعی مستقل به خارج از سازمان مقدور نمی‌باشد، مرکز فرماندهی، به‌عنوان رده هماهنگ‌کننده با مرکز ماهر و دیگر آپاها نقش ایفا خواهد نمود. در این مدل یکی از نکاتی که با مراکز غیر دفاعی به چشم می‌خورد بحث سلسله مراتبی است؛ مراکز دفاعی به‌واسطه نوع ماموریتی که دارند باید سلسله‌مراتب را رعایت نموده و در مواردی که رخدادی به وجود می‌آید باید حتما به رده‌بالا دستی خود گزارش دهند و نمی‌توانند که بدون

هماهنگی با تیم‌های دیگر سازمان‌ها، ارتباط داشته باشند؛ ضمن اینکه به‌کارگیری از سامانه‌های بلادرنگ و چابک که مختص مراکز دفاعی است باید استفاده گردد.




شکل ۳: نمایش مدل تیم پاسخ‌گویی مراکز دفاعی و ارتباط لایه‌ها با یکدیگر و مرکز ماهر

با توجه به پراکندگی و نیاز به داشتن یکپارچگی در ماموریت و انسجام بیشتر، پاسخگویی سریع به رخدادها، مسوولیت متمرکز و تلفیقی و همچنین پشتیبانی بهتر زیرمجموعه‌ها و با توجه به نقاط قوت و ضعف مدل‌ها، مدل ترکیبی (ادغام متمرکز و توزیع‌پذیر) را می‌توان برای مراکز دفاعی و زیرمجموعه‌های تابعه آن مطابق با شکل (۳) در نظر گرفت. هرچند که مدل متمرکز نیز تا حدی می‌توانست برای مراکز دفاعی مناسب باشد ولی به علت پراکندگی نقاط، اتلاف زمان برای شناسایی و از بین بردن رخداد این گزینه منتفی است. لذا مدل ترکیبی که برای سازمان‌های بزرگ و پراکنده به بهترین نحو عمل می‌کند و دارای ویژگی‌هایی است که سازگاری آن با وضعیت مراکز دفاعی مطابقت دارد. فرماندهی دفاعی با توجه به تمرکز مدیریت، به‌عنوان تیم پاسخ‌گویی هماهنگ‌کننده برای برقراری ارتباط بین تیم‌های پاسخ‌گویی مراکز عمده دفاعی و دیگر زیرمجموعه‌ها پیشنهاد می‌گردد. همچنین ویژگی‌های عمده مدل ترکیبی در مراکز دفاعی عبارت‌اند از:

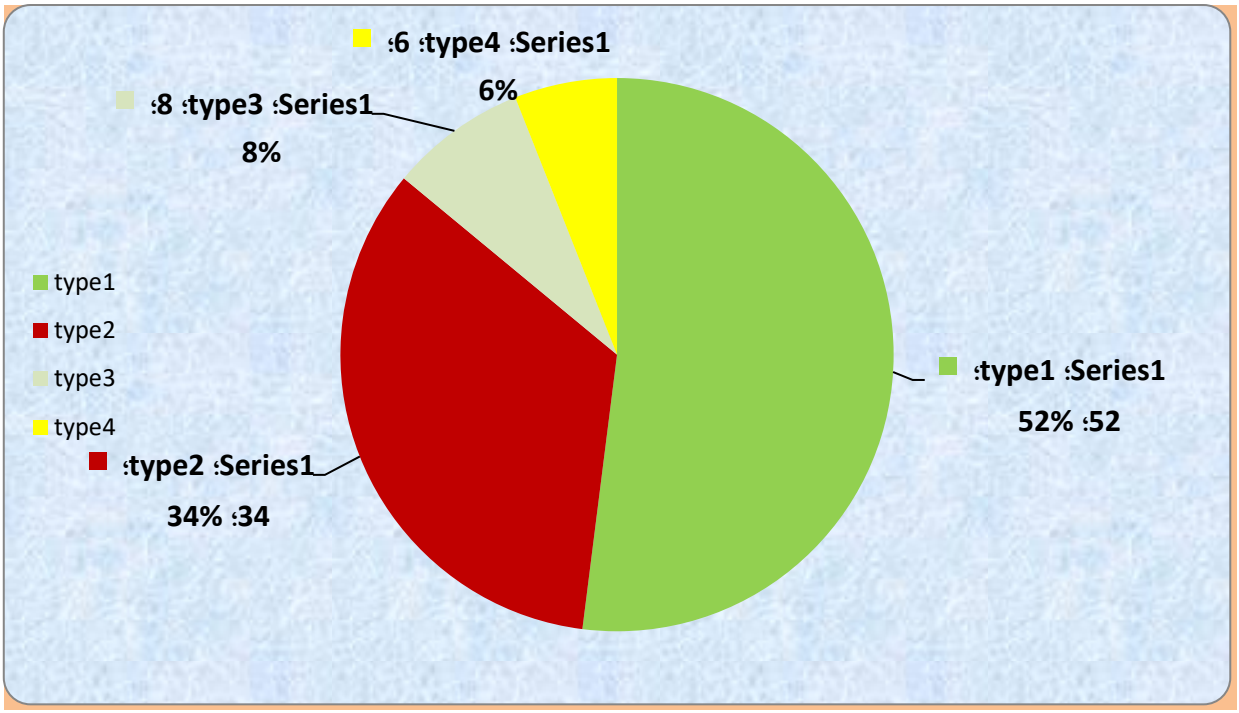
- تشکیل بخش متمرکز تیم پاسخ‌گویی به‌صورت هسته‌ای پایدار از افراد متخصص،
- توزیع تعدادی از کارمندان موجود در موقعیت‌های راهبردی سازمان و دیگر زیرمجموعه‌ها،
- جمع‌آوری، ترکیب و پیگیری تمامی گزارش‌ها توسط اعضای تیم مرکزی،

- تحلیل مناسب و کارا و تدوین راهبردهای مهار رخدادها توسط تیم مرکزی،
- پیاده‌سازی راهبردهای تدوین‌شده در هسته مرکزی، توسط اعضای پراکنده تیم،

- پاسخ‌گویی سریع‌تر به‌رخدادها توسط اعضای توزیع‌شده تیم در سطح مراکز دفاعی،
- انتقال مهارت و دانش به‌حوزه‌های مسئولیت توسط اعضای پراکنده تیم.

### ۱۱-۲- تعیین فرآیند گزارش‌گیری (تریاژ)

برای دریافت گزارش و فرآیند دسته‌بندی و ارسال گزارشات برحسب اولویت چهار نوع دسته‌بندی برای آن وجود دارد که در روش اول تمامی گزارشات به مرکز واردشده و پس از دسته‌بندی و اولویت‌گذاری به تیم توزیع‌شده واگذار می‌شود. در روش دوم گزارشات به سایت‌های توزیع‌شده می‌روند و گزارش‌گیری اولیه در آنجا انجام می‌شود و در صورت عدم امکان رسیدگی به آن‌ها در قسمت‌های توزیع‌شده به تیم مرکزی ارسال می‌شوند. در روش سوم تیم متمرکز تنها گزارش‌های رخدادها را دریافت کند و کار تحلیل و پاسخ‌گویی را با توجه به مهارت‌ها و موقعیت جغرافیایی اعضای تیم توزیع‌شده، به افراد مناسبی از آن‌ها محول می‌کند و در روش چهارم از روش اولین ورودی اولین خروجی[1] برای اولویت‌گذاری گزارش‌های حوادث و درخواست‌های تیم پاسخ‌گویی استفاده می‌شود که در نظرسنجی‌های صورت گرفته روش اول ۵۲٪ و روش دوم ۳۴٪، روش سوم ۸٪ و روش چهارم ۶٪ انتخاب شد. شکل شماره (٤) نظرسنجی تریاژ تیم پاسخ‌گویی دفاعی نشان داده‌شده است.

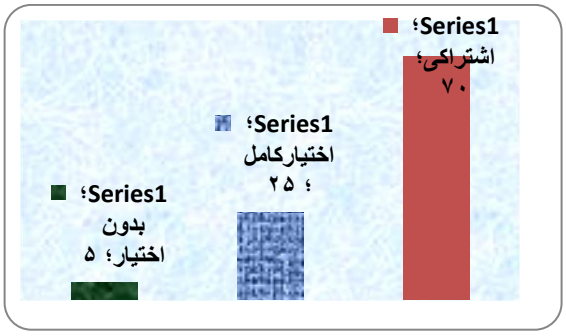



۱- First In First Out(FIFO).

شکل ۴: نظرسنجی تریاژ تیم پاسخ‌گویی

## ۱۱-۳- تعیین میزان اختیارات تیم پاسخ‌گویی مراکز دفاعی

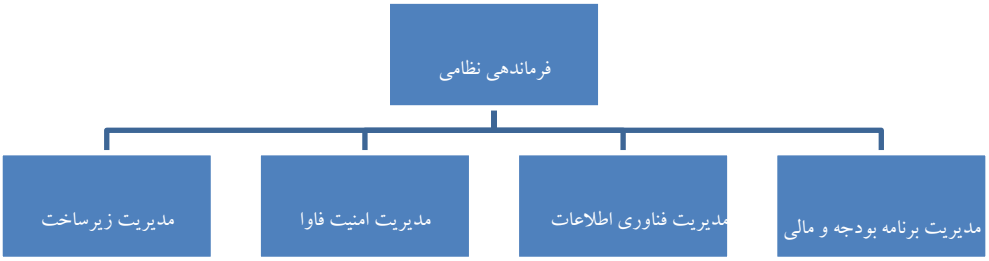
یکی دیگر از مواردی که باید به آن توجه نمود میزان اختیاراتی است که تیم پاسخ‌گویی دفاعی دارد. در این تصمیم‌گیری باید اختیار تیم پاسخ‌گویی را از بین سه دسته اختیار کامل، اختیار مشارکتی و فقدان اختیار انتخاب نمود. در سازمان‌های دفاعی با توجه به این‌که تمامی دستورات و فرامین باید فرآیند خاصی را طی نمایند، لذا داشتن اختیار کامل برای تیم پاسخ‌گویی دفاعی ممکن نیست؛ همچنین در صورت نداشتن اختیار، تیم پاسخ‌گویی عملاً در مجموعه فقط به سرویس هشدار دهی و اعلان پیام‌های امنیتی محدود خواهد شد؛ لذا اگر تیم ترکیبی، اختیار کاملی در تحلیل فعالیت‌ها داشته باشد و برای پاسخ‌گویی به رخدادها دارای اختیار اشتراکی باشد، عملکرد بهتری خواهد داشت. بنابراین در تیم پاسخ‌گویی دفاعی که دارای اختیار اشتراکی می‌باشد بهتر است در مسایل تحلیل آسیب‌پذیری‌ها دارای اختیار کامل بوده ولی در مسایلی مانند بازیابی راهبردها و مسایل مهم دیگر با ابلاغ مسئولین و فرماندهان انجام‌پذیر باشد. با توجه به پرسش‌نامه‌های صورت گرفته، اکثر خبرگان نیز به‌انجام این مأموریت با داشتن اختیار اشتراکی موافق بودند. در این تصمیم‌گیری پاسخ‌دهندگان به ۷۰٪ اختیار اشتراکی، ۲۵٪ اختیار کامل و ۵٪ بدون اختیار رای دادند. شکل شماره (۵) نظرسنجی میزان اختیارات تیم پاسخ‌گویی دفاعی نشان داده‌شده است.




شکل ۵: نظرسنجی در مورد میزان اختیار و اقتدار تیم پاسخ‌گویی

## ۱۱-٤- مشارکت‌کنندگان در راه‌اندازی تیم پاسخ‌گویی فوریت رایانه‌ای دفاعی

با توجه به‌نظر خبرگان، بخش‌های که در راه‌اندازی تیم پاسخ‌گویی مراکز دفاعی نقش‌آفرینی می‌کنند به‌صورت شکل (٦) می‌باشند:




شکل ۶: بخش‌های مرتبط در ایجاد تیم پاسخ‌گویی ترکیبی دفاعی

## ۱۱-۵- تعیین سرویس‌های موردنیاز

برای ایجاد یک تیم پاسخ‌گویی ترکیبی، خدماتی که تیم پاسخ‌گویی ترکیبی باید ارائه دهد به دو قسمت خدمات اصلی و خدمات اضافی تقسیم می‌شوند؛ هرچند که پیشنهاد می‌شود در مراحل ابتدایی و آغازین، رویس‌های اضافی راه‌اندازی نشود ولی در صورت داشتن شرایط لازم بلامانع است. این سرویس‌ها در جدول (٦) ارایه گردیده است.

جدول ۶: سرویس‌های ارائه‌شده تیم پاسخ‌گویی رده‌ها (مدل ترکیبی)

| ردیف | سرویس‌های اصلی | قابلیت |
|---|---|---|
| ۱ | هشدارها و اخطارها | √ |
| ۲ | تحلیل رخداد | √ |
| ۳ | پشتیبانی پاسخ‌گویی به رخداد | √ |
| ۴ | هماهنگی در پاسخ‌گویی به رخداد | √ |
| ۵ | هماهنگی در پاسخ‌گویی به حفره‌های امنیتی و آثار باقی‌مانده | √ |
| ۶ | اعلان‌ها | √ |
| ۷ | پایش فناوری | √ |
| ۸ | انتشار اطلاعات مرتبط با امنیت | √ |
| ردیف | **سرویس‌های اضافی** | **قابلیت** |
| ۱ | پاسخ‌گویی به رخداد در محل | √ |
| ۲ | سرویس‌های تشخیص نفوذ | √ |
| ۳ | تحلیل حفره‌های امنیتی و آثار باقی‌مانده از حمله | √ |
| ۴ | ممیزی یا ارزیابی امنیتی | √ |
| ۵ | تنظیم، پیکربندی و نگهداری ابزارها، نرم‌افزارها و زیرساخت‌های امنیتی | √ |
| ۶ | توسعه ابزارهای امنیتی | √ |

## ۱۱-٦- بخش‌های موردنیاز تیم پاسخ‌گویی دفاعی

سرویس‌های مورد نیاز اعم از اصلی و اضافی بخش‌های تعریف شده باید سرویس‌های مرتبط با مدل ارایه شده را پوشش دهند؛ بخش‌های موردنیاز برای تیم پاسخ‌گویی دفاعی به ٤ بخش عمده تقسیم می‌شود:

### ۱۱-٦-۱- بخش اجرایی و پاسخ‌گویی

این بخش خدمات مربوط به‌سرویس‌های زیر را انجام می‌دهد:

۱. پشتیبانی پاسخ‌گویی به‌رخداد، ۲. هماهنگی در پاسخ‌گویی به‌رخداد، ۳. هماهنگی در پاسخ‌گویی به حفره‌های امنیتی و آثار باقی‌مانده، ٤. پاسخ‌گویی به‌رخداد در محل.

### ۱۱-٦-۲- بخش تحلیل مخاطرات و ارزیابی

این بخش نیز سرویس‌هایی را که پیرامون تحلیل فنی مخاطرات می‌باشد را پشتیبانی نموده و شامل خدمات زیر می‌باشد: ۱. هشدارها و اخطارها، ۲. تحلیل رخداد، ۳. سرویس‌های تشخیص نفوذ، ٤. تحلیل حفره‌های امنیتی و آثار باقی‌مانده از حمله، ۵. ممیزی یا ارزیابی امنیتی.

### ۱۱-٦-۳- بخش آموزش و تولید محتوا

در این بخش مدل تیم پاسخ‌گویی ترکیبی با داشتن یک گروه متمرکز و اختصاصی می‌تواند روی ارسال اطلاعات مرتبط با امنیت برای بقیه سازمان نیز تمرکز نماید. لذا در حالت کلی سرویس‌های زیر مربوط به بخش آموزش می‌باشد: ۱. اعلان‌ها، ۲. پایش فناوری، ۳. انتشار اطلاعات مرتبط با امنیت.

### ۱۱-٦-٤- بخش پشتیبانی

سرویس‌های زیر مربوط به بخش پشتیبانی می‌باشد:

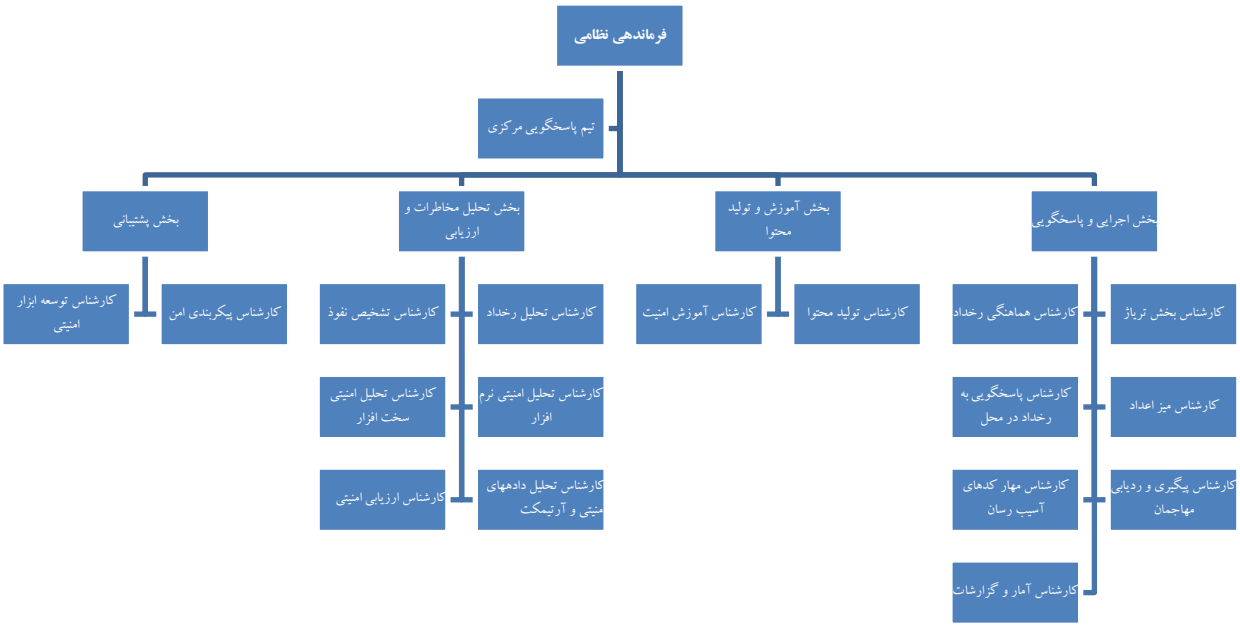
- تنظیم، پیکربندی و نگهداری ابزارها، نرم افزارها و زیرساخت‌های امنیتی،
- توسعه ابزارهای امنیتی.
- در جدول (۷) بخش‌ها و سرویس‌های قابل ارایه در تیم پاسخ‌گویی دفاعی ارایه گردیده است.

جدول ۷: بخش‌ها و سرویس‌های ارائه‌شده در تیم پاسخ‌گویی ترکیبی

| ردیف | بخش‌های تیم‌های پاسخ‌گویی | سرویس‌ها |
|---|---|---|
| ۱ | بخش اجرایی و پاسخ‌گویی | • پشتیبانی پاسخگویی به رخداد<br>• هماهنگی در پاسخگویی به رخداد<br>• هماهنگی در پاسخگویی به حفره‌های امنیتی و آثار باقیمانده<br>• پاسخگویی به رخداد در محل |
| ۲ | بخش تحلیل مخاطرات و ارزیابی | • هشدارها و اخطارها<br>• تحلیل رخداد<br>• سرویس‌های تشخیص نفوذ<br>• تحلیل حفره‌های امنیتی و آثار باقی‌مانده از حمله<br>• ممیزی یا ارزیابی امنیتی |
| ۳ | بخش آموزش و تولید محتوا | • اعلان‌ها<br>• پایش فناوری<br>• انتشار اطلاعات مرتبط با امنیت |
| ۴ | بخش پشتیبانی | • تنظیم، پیکربندی و نگهداری ابزارها، نرم‌افزارها و زیرساخت‌های امنیتی<br>• توسعه ابزارهای امنیتی |

## ۱۱-۷- جایگاه و چارت سازمانی

تیم پاسخ‌گویی بنا به‌موقعیت می‌تواند جایگاه مختلفی داشته باشد، تیم پاسخ‌گویی از نظر جایگاه ساختمانی می‌تواند در موقعیت‌های متفاوتی قرار گیرد. می‌تواند درون بخش‌های فناوری اطلاعات یا بخش امنیت و حتی در بخش زیرساخت به‌عنوان یک واحد باشد یا اینکه می‌تواند به‌عنوان یک بخش مستقل زیر نظر مستقیم فرماندهی قرار گیرد و این بسته به‌اقتداری است که در سازمان برای آن تعریف می‌شود. به‌عنوان‌مثال تیم پاسخ‌گویی ایالات‌متحده با توجه به نفوذ خود می‌تواند ارتش را به‌عکس العمل‌هایی وادار کند. در تیم پاسخ‌گویی دفاعی با توجه به‌گستردگی و اختیار مشارکتی بهتر است که بخشی مستقل زیر نظر فرماندهی بوده و اجزاء تشکیل یافته یا همان چارت سازمانی به‌صورت پیشنهادی شکل (۷) بر اساس تعداد موردنیاز برای مدل ترکیبی تیم پاسخ‌گویی ارایه می‌نماید؛ نکته مهم در جایگاه سازمانی مراکز دفاعی این است که مراکز دفاعی از نوع سلسله مراتبی هستند و ویژگی دوم این است که این مراکز باید چابک باشند و این دو ویژگی عمده، متمایزکننده از بخش‌های غیر دفاعی است.




شکل ۷: جایگاه و چارت پیشنهادی تیم پاسخ‌گویی دفاعی

## ۱۲- نتیجه‌گیری

در این مقاله پس از تبیین مفاهیم تیم پاسخ‌گویی، مدل‌ها، سرویس‌ها و خدمات تیم پاسخ‌گویی و دیگر مولفه‌ها و موارد اثرگذار در تیم پاسخ‌گویی موردبررسی قرار گردید؛ سپس در پیشینه تحقیق، چند نمونه از تیم‌های پاسخ‌گویی دفاعی و غیر دفاعی مهم دنیا موردبررسی قرار گرفت و اهداف آن‌ها از به‌کارگیری تیم پاسخ‌گویی بیان گردید؛ در پیشینه تحقیق با توجه به‌ضرورت تخلیص، امکان معرفی فعالیت سایر کشورها در این حوزه وجود نداشت؛ ولکن در این حوزه، اکثر کشورها، فعالیت‌های مناسب و گام‌های بزرگی را برداشته‌اند و توانسته‌اند که با سازوکار مناسب، امنیت شبکه‌ها و زیرساخت سایبری خود را ارتقاء دهند؛ نقاط قوت و ضعف مدل‌های استقرار تیم‌های پاسخ‌گویی موردبررسی قرار گرفت و پس از بررسی همه جوانب امر درنهایت، پس از اجماع نظر خبرگان دفاعی در حوزه

سایبری و تحلیل آماری، مدل مفهومی تیم پاسخ‌گویی دفاعی، سرویس‌ها و جایگاه و دیگر موارد مهم تیم پاسخ‌گویی دفاعی پیشنهاد گردید؛ مدل ترکیبی که آمیخته‌ای از مدل متمرکز و توزیع‌شده است، از نتایج این تحقیق برای تیم پاسخ‌گویی فوریتی دفاعی است؛ از طرفی اختیار اشتراکی و روش دسته‌بندی رخدادها در تریاژ که در آن تمامی گزارشات به مرکز وارد شده و پس از دسته‌بندی و اولویت‌گذاری به تیم توزیع‌شده واگذار می‌شود و سرویس‌های مورد ارایه مدل ترکیبی از دیگر نتایج این تحقیق است؛ و درنهایت ساختار و سازمان این تیم در این تحقیق ارایه گردید؛ حفظ انسجام بین لایه‌های ارتباطی و رده‌ها و نیز آموزش و فرهنگ‌سازی بین کارمندان، از دیگر موارد مهم، قبل از ایجاد تیم پاسخ‌گویی فوریتی است؛ تمامی موارد ذکرشده، نتایج بررسی یک تحقیق علمی است، وجود ساختار سلسله مراتبی، چابکی، استفاده از سامانه بلادرنگ از موارد بارز و متفاوت با تیم پاسخ‌گویی غیر دفاعی است که در مدل پیشنهادی تشریح گردید؛ اما نکته مهمی که در اکثر مقالات به‌صورت مغفول باقی می‌ماند، جلب نظر مدیران و مسئولان راهبردی و تصمیم گیر است و بدون همراهی آن‌ها پیاده‌سازی تیم پاسخ‌گویی فوریتی رایانه‌ای میسر نخواهد شد؛ لذا امید است بامطالعه این تحقیق، مدیران و مسئولان تصمیم گیر ن.م در سطح راهبردی به‌ضرورت و اهمیت راه‌اندازی تیم پاسخ‌گویی فوریتی رایانه‌ای بالأخص در مراکز دفاعی پی برده و آن را از اولویت‌های اصلی سازمان قرار دهند.

## ۱۳- فهرست منابع و مآخذ


- رشتی، سید محمدرضا. (۱۳۸۸). ***راهنمای ایجاد یک تیم پاسخ‌گویی به رخدادهای امنیتی رایانه‌ای CSIRT***. تهران: رویش جوانه‌های فردا.
- سازمان پدافند غیرعامل کشور. (۱۳۹۳). «***بررسی و ارزیابی ریسک‌ها و مخاطرات سایبری***».
- سند نظام ملی پیشگیری و مقابله با رخدادهای فضای مجازی.
- صیاد، محمدکاظم و امینی، آرمین و طاهری، ابوالقاسم. (۱۳۹۹). «***تهدیدات سایبری و اقدامات امنیتی در فضای مجازی***» فصلنامه علمی امنیت ملی، سال دهم، شماره سی و هشتم.
- طیرانی، احسان. (۱۳۹۵). ***مدیریت رخدادهای امنیت رایانه‌ای و تشکیل تیم‌های CERT سازمانی***، آپای مشهد.
- کشاورز، رضا. (۱۳۹۳). «***ارایه الگوی استقرار CERT مراکز نظامی***»، مجله علمی پژوهش‌های حفاظتی.
- علیدوستی، میترا. (۱۳۹۲). «***بررسی الگوریتم‌ها و روش‌های تست نفوذ و ارزیابی ابزارهای موجود***»، پایان‌نامه کارشناسی ارشد مهندسی رایانه گرایش معماری سیستم‌های رایانه، دانشگاه علم و صنعت.
- Alberts, Chris. Dorofee, Audrey. Killcrece, Georgia. Ruefle, Robin. Zajicek, Mark. (۲۰۱۶). "***Defining Incident Management Processes for CSIRTs: A Work in Progress***". U.S: Software Engineering Institute, Carnegie Mellon University.
- Brownlee, N. (۲۰۱۸). "***Expectations for Computer Security Incident Respons***". U.S: Software Engineering Institute, Carnegie Mellon University.
- Blueprint for a Secure Cyber Future: (۲۰۱۷)***The Cybersecurity Strategy forthe Homeland Security Enterprise NIST Incident Response***, ۲۰۲۱, The step bysetp guide for incident response reporting.

- DOD Faces Challenges In Its Cyber Activities, July (۲۰۱۷)
- John Franco Dept, (۲۰۱۷) ***Cyber Defense Overview Electrical Engineering and Computing Science.***
- Killcrece, Georgia. Kossakowski, Klaus-Peter. Ruefle, Robin. Zajicek, Mark. (۲۰۱٦) "***State of the Practice of Computer Security Incident Response Teams (CSIRTs)***". US: Carnegie Mellon University.
- Kossakowski, Klaus-Peter, Robin Ruefle,Mark Zajicek.(۲۰۱۷) ."***Organizational Models for Computer Security Incident ResponseTeams (CSIRTs)***.*"* US: Software Engineering Institute, Carnegie Mellon University.
- Martijn van der heide (۲۰۱۷), ***Management strategies for implementing forensic security measures***
- Penedo, David. (۲۰۱٦). "***Technical Infrastructure of a CSIRT***". Cote d'Azur: Internet Surveillance and Protection, ICISP". US: Software Engineering Institute, Carnegie Mellon University.
- Sally Brice-O Hara, ***Coast Guard IntelligenceJan***, (۲۰۱۷).
- Scarfone, Karen. Grance, Tim and Masone, Kell. (March ۲۰۱۸). "***Computer Security Incident Handling Guide***". U.S: Department of Commerce, National Institute of Standards and Technology.

- سایت اینترنتی تیم پاسخ‌گویی فوریتی مرکز ماهر
- سایت اینترنتی پلیس فتا

- WWW.CERT.ORG
- WWW.CERT.IR
- WWW.Itlaw.wikia.org