فصلنامه مطالعات جنگ
سال سوم، شماره نهم، تابستان ۱۴۰۰
مقالهٔ اول از صفحه ۵ تا ۲۶

ارایه مدل پیشنهادی CERT سازمان‌های دفاعی به‌منظور کاهش تهدیدات سایبری

رضا کشاورز *[۱]، محمدرضا موحدی صفت[۲]

دریافت مقاله: ۱۴۰۰/۰۴/۰۹ پذیرش مقاله:۱۴۰۰/۰۵/۱۲

چکیده

یکی از مهمترین نکات در هنگام بروز رخدادهای امنیتی برای یک سازمان نظامی آن است که شیوه پاسخ‌گویی مناسب به آن رخداد را بداند. در واقع سرعت در تشخیص، تحلیل و پاسخ‌گویی به یک مشکل امنیتی، میزان خطر و هزینه ترمیم را کاهش می‌دهد. CERT که تیم پاسخ‌گویی فوریتی رایانه‌ای می‌باشد وظیفه پشتیبانی و سرویس‌دهی به‌منظور پیش‌گیری، پاسخ‌گویی و برطرف کردن رخدادهای رایانه‌ای از قبیل سرویس‌های مخرب، انتشار بد افزارها، دسترسی‌های غیرمجاز، بکارگیری نامناسب و حملات ترکیبی را بر عهده دارد. برای اینکه پاسخ‌گویی به رخدادهای پیش‌آمده در کمترین زمان ممکن صورت پذیرد، راه‌اندازی یک CERT مطمئن در مراکز نظامی امری ضروری است؛ به‌طوری‌که در یک بستر قابل اطمینان بتوان شبکه را کنترل نمود و حملات و نفوذهای غیر مجاز را تشخیص داد و در کم‌ترین زمان ممکن با ارتباط بهینه بین اجزاء، سرعت پاسخ‌گویی را بالا برد؛ لذا وجود CERT در این سازمان‌ها از مسائل راهبردی محسوب می‌شود. در این تحقیق با مطالعات انجام شده و بهره‌گیری از نظر خبرگان نظامی در حوزه سایبری و تحلیل نتایج آماری، مدل پیشنهادی CERT نظامی هیبریدی(ترکیبی)، خدمات و سرویس‌های قابل ارایه، جایگاه و میزان اقتدار و چارت سازمانی CERT مراکز نظامی ارایه می‌گردد.

واژگان کلیدی: تیم پاسخ‌گویی فوریتی رایانه‌ای، شیوه پاسخ‌گویی، مدل پیشنهادی CERT نظامی ترکیبی.

۱ - دانشجوی دکتری امنیت سایبری دانشگاه عالی دفاع ملی(Rezakeshavarz@sndu.ac.ir) - نویسنده مسئول (۰۹۱۹۴۵۸۰۸۹۹)
۲ -استادیار و عضو هیات علمی دانشگاه عالی دفاع ملی، movahedi@sndu.ac.ir

مقدمه

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 قرار گرفته‌اند. این دارایی‌ها همواره در معرض تهدیدات و آسیب‌پذیری‌های جدی قرار دارند. حملات سایبری در محیط شبکه‌های سازمانی روز به روز در حال افزایش هستند و ممکن است در یک بازه زمانی بسیار کوتاه کل 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 هزینه ترمیم را کاهش می‌دهد. تیم پاسخ‌گویی فوریتی به حوادث رایانه‌ای[1]، یک سازمان خدماتی است که مسئول دریافت، مرور و پاسخ‌گویی به گزارشات ارسالی و فعالیت‌های مربوط به مشکلات و رویدادهای رایانه‌ای است(دیوید و پندو، ۲۰۰۶). در واقع CERT یک نقطه مرکزی برای گزارشات مرتبط با مشکلات امنیتی است که پس از بررسی اطلاعات وارد شده، الگو و هدف فعالیت مخرب در آن شناسایی گردیده و عکس العمل مناسب نشان داده می‌شود. CERT می‌تواند با سایر تیم‌های پاسخ‌گویی به حوادث رایانه‌ای در خارج سازمان همکاری داشته باشد. این همکاری به اشتراک راهبردها در پاسخ‌گویی به حملات مشابه می‌انجامد و به عنوان یک هشداردهنده برای مشکلات بالقوه است (براون، استیکورت، ۲۰۱۰).

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. CERT 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 نظر گرفته می‌شود (دیوید و پندو، ۲۰۰۶).

با توجه به تأکیدات مقام معظم رهبری، مفاد صریح و اسناد بالادستی مبنی بر دست‌یابی و ارتقاء قدرت سایبری کشور در تراز قدرت‌های جهانی و برای حضور پرقدرت و باصلابت در فضای مدیریتی و حاکمیتی این فضا باید به موضوع امنیت و مقابله با تهدیدات توجه کافی و جدی شود؛

1.1.1. [1] CERT: Computer Emergency Response Team

به همین منظور رویه‌ها و روش‌های مناسب جهت پاسخ‌گویی به تهدیدات و رخدادهای زیرساختی نیازمند مرجع مناسب وشیوه نامه منسجمی می‌باشد. این امر موجب افزایش تاب آوری در برابر تهدیدات و ایجاد خسارات جبران ناپذیری خواهد شد؛ لذا وجود CERT در سازمان‌های دفاعی و ایجاد انسجام در هماهنگی بین بخش‌های مختلف آن در مواجهه با تهدیدات امنیتی زیرساخت‌های سایبری، از مسائل راهبردی سازمان‌های دفاعی و مسئله اصلی این تحقیق است.

با انجام این تحقیق و در صورت ترغیب سیاستمداران برای ایجاد CERT سازمان‌های مسلح، شاهد افزایش انعطاف‌پذیری و آمادگی در برابر تهدیدات سایبری، کاهش خسارات و صدمات به زیرساخت‌ها، تجهیزات و سامانه‌ها، اطلاع از وضعیت موجود شبکه و سامانه‌های رایانه‌ای و شناسایی زود هنگام تهدیدات سایبری خواهیم بود؛ از طرفی تاکنون تحقیقی مستقل در خصوص راهبردهای بکارگیری CERT در سازمان‌های دفاعی انجام نشده است و لذا در این تحقیق، درک و فهم بهتری جهت ارایه طرح و برنامه‌های انفعالی در مواقع برخورد با رویدادهای سایبری بیان شده است.

در فرآیند مطالعات پیشین، متدولوژی به عنوان قسمتی از یک چارچوب مدیریتی مناسب برای شناسایی و ارزیابی فرآیند مورد نیاز است؛ به همین منظور در مقاله‌ای با عنوان "ارایه الگوی استقرار CERT مراکز نظامی"، روش پاسخ‌گویی به حوادث از دیدگاه‌های NIST[1] و SEI[2] و JPCERT[3] را مورد بررسی قرار داده است؛ همچنین تطبیق مدل‌های CERT در پاسخ‌گویی به حوادث، سرویس‌ها و ساختارهای پیشنهادی مراکز نظامی، الگوی فرآیند نحوه مقابله تیم CERT در مراکز نظامی با یک رخداد و ارتباط بین مولفه‌ها در این مقاله بررسی شده و در نهایت مدل استقرار CERT مراکز نظامی ارایه گردیده است (کشاورز رضا، ۱۳۹۲). همچنین در نشریه‌ای از آپای دانشگاه فردوسی مشهد،آقای طیرانی به بررسی انواع CERTها پرداخته و روش‌های مقابله با رخدادهای رایانه‌ای و بررسی نقاط قوت و ضعف انواع CERT را مورد بررسی قرار داده است و این موارد از نقاط اشتراک این مقاله با موضوع مورد تحقیق می‌باشد (طیرانی احسان، ۱۳۹۵). پرداختن به خدمات CERT، خدمات مدیریت کیفیت امنیت و اندازه تیم و تعداد نفرات از دیگر موارد مورد نیاز در مطالعه CERT می‌باشند که آقای رشتی با عنوان ایجاد یک تیم پاسخ‌گویی به

[1] *National Institute of standard and technology*

[2] *Software Engineering Institute*

[3] *jappanices CERT*

رخدادهای رایانه‌ای به این مسأله پرداخته است (رشتی، سیدمحمدرضا و همکاران، ۱۳۹۲). مدیریت مخاطرات و آنالیز موقعیتی و مکانی از دیگر موارد مورد تفحص شده در نشریه سایبر ملی می‌باشند (National Cyber Incident Response Plan، ۲۰۱۷). همچنین معماری و اجزای لایه معماری CERT نیز به عنوان یکی از مهمترین مؤلفه‌ها در بررسی یک CERT از سند سایبر ملی مورد استفاده قرار گرفته است (Home land security، ۲۰۱۶).

هدف این تحقیق، ارائه مدل‌هایی جهت بکارگیری CERT سازمان‌های دفاعی در برابر کاهش تهدیدات سایبری است و تلاش در راستای آگاهی بخشیدن و ارایه شناخت کافی به مخاطبان جهت پیاده‌سازی CERT، روش بکارگیری CERT سازمان‌های دفاعی و تاثیر ایجاد این ساختار بر کاهش تهدیدات سایبری در مراکز دفاعی است.

این تحقیق از حیث هدف تحقیقی کاربردی؛ از حیث سطح تحلیل برخوردار از ماهیتی توصیفی– استنباطی و از حیث رویکرد و طبقه‌بندی روش متکی به روش کتابخانه‌ای می‌باشد. داده‌های مورد نیاز از راه مطالعات کتابخانه‌ای و با استفاده از ابزار فیش‌برداری گردآوری شده است و با نظر خبرگان حوزه سایبری نظامی، سوالاتی تنظیم شده است و پس از توزیع سوالات در بین افراد جامعه هدف، نتایج آن از طریق نرم‌افزار spss ، به‌عنوان نتایج تحقیق ارایه شده است.

مبانی نظری

۱–۲– تعریف رویدادها[1] و حوادث رایانه‌ی[2]

برای سازمان‌دهی قابلیت پاسخ‌گویی به حوادث رایانه‌ای چند جنبه مهم باید تعریف گردد: یکی از آن‌ها تعریف واژه حادثه است. هر اتفاق قابل مشاهده 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[3] دارای پیامد منفی است مثل طغیان بسته‌های شبکه، هنگ‌کردن سیستم، استفاده غیرمجاز از داده‌های حساس و غیره. حوادث امنیتی رایانه‌ی[4] شامل تهدید حتمی به خط‌مشی امنیتی رایانه‌ای است. یک حادثه به‌دلایل فراوانی ممکن است اتفاق بیفتد؛ بنابراین ارایه یک رویه جامع با یک دستورالعمل مرحله به مرحله برای هر نوع حادثه‌ای غیرممکن است پس بهتر است به بحث در

---

[6]- Event
[7]- Incident
[3] -Adverse events
[4] -computer security incident

خصوص حوادث رایج پرداخته شود. طبقه‌بندی حوادث که در ادامه به آن ارائه شده یک دسته بندی اولیه می‌باشد:

أ. **از کار اندازی سرویس**[1]: 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 را دارند 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 ICMP به شبکه استفاده می‌کند که منجر به از کار افتادن آن می‌شود.

ب. **انتشار بدافزارها**[2]: 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 ضد ویروس اخطاری دریافت کند مبنی بر این‌که ویروس جدیدی به سرعت از طریق پست الکترونیک در اینترنت پخش می‌شود. این ویروس از آسیب‌پذیری که هم اکنون در بسیاری از میزبان‌های سازمان وجود دارد، بهره می‌برد. از این‌رو انتظار می‌رود در زمان اندکی تعدادی از میزبان‌ها آلوده شوند.

ج. **دسترسی غیرمجاز**[3]: هنگامی که 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 به‌دست می‌آورد.

د. **استفاده نامناسب**[4]: 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**: با تقسیم‌کردن حوادث به دسته‌های معین و ارائه راهنمایی‌هایی برای تشخیص، تحلیل و پاسخگویی به هر یک از انواع حوادث می‌توان پاسخگویی را به نحو

---

[1] -Denial of Service(DOS)
[2] -Malicious Code
[3] -Unauthorized Access
[4] -Inappropriate Usage

موثرتری انجام داد. طبقه‌بندی کردن فقط با مشخص کردن نوع حادثه‌ای که گزارش شده است انجام نمی‌شود بلکه شامل تعیین رابطه حادثه با دیگر حوادث نیز هست. به عنوان مثال 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، تیام، کیل، ۲۰۰۸).

۲-۲- بررسی برخی از CERTهای فعال در عرصه جهانی

امروزه کشورهای فراوانی موفق به راه‌اندازی CERT شده‌اند و آن را در لایه‌های مختلف مدیریتی و زیرساختی به‌کارگیری نموده‌اند؛ در این مقاله دو کشور آمریکا و کره جنوبی مورد بررسی قرار گرفته‌اند.

۱- آمریکا

کشور 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 سال۲۰۰۱، مورد بازنگری 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 تعیین شده‌اند:

۱) جلوگیری از حملات علیه زیرساخت‌های اطلاعاتی حیاتی کشور،

۲) کاهش نفوذ پذیری‌ها،

۳) به حداقل رساندن خسارات و زمان احیاء.

ایالات متحده آمریکا به عنوان پیش‌گام در این موضوع، اولین CERT را در سال ۱۹۸۹ در دانشگاه کارنگی ملون ایجاد نمود و همچنین برای راه اندازی CERT و منابع آموزشی، سایت www.CERT.org را ایجاد نمود که بهترین مرجع اینترنتی در این حوزه می‌باشد (رشتی رضا، رشتی زهرا، سیفی مهدی،۱۳۹۲،ص ۸-۱۲).

۲- کره جنوبی

کره جنوبی جزو کشورهای نسبتاً پیشرفته محسوب می‌شود. در سال ۱۹۹۶ KRCERT شکل گرفت و هم‌اکنون نیز به عنوان تیم مقابله با حوادث در سطح ملی ایفای نقش می‌نماید. با توجه به بازبینی وضعیت حملات ویروسی و نفوذهای امنیتی در سال ۲۰۰۰ و تحلیل اثرات مخرب این حملات بر زیرساخت‌های ارتباطی و اطلاعاتی کشور، قانون حفاظت از زیرساخت‌های اطلاعاتی و ارتباطی در سال ۲۰۰۱ به تصویب رسید و کمیته محافظت از زیرساخت‌های ارتباطی تشکیل شد.

بر اساس قانون حفاظت از زیرساخت‌های اطلاعاتی و ارتباطی کره جنوبی:

- دولت می‌تواند زیرساخت‌های اطلاعاتی کلیدی را حتی در بخش تجاری شناسایی کند.
- در زیرساخت‌هایی اطلاعاتی که کلیدی شناخته می‌شوند باید مبانی امنیتی محکمی اعمال شود و آسیب‌پذیری‌های احتمالی آن‌ها ارزیابی شود.
- حملات به زیرساخت‌های اطلاعاتی کلیدی باید به سازمان‌های اعمال قانون، یا ((آژانس امنیت اطلاعات کره)) یا ((موسسه تحقیقات ارتباطات و الکترونیک)) گزارش شوند.
- شرکت‌های خاصی می‌توانند توسط دولت برای ارزیابی زیرساخت‌های اطلاعاتی حیاتی به کار گرفته شوند.
- ((مرکز تحلیل و اشتراک اطلاعات)) و سیستم‌های مدیریت امنیت اطلاعات توسط این قانون پوشش داده می‌شوند(همان).

۳- مدل‌ها و خدمات مهم CERT

در این بخش به مدل‌ها، خدمات، جایگاه سازمانی، میزان اقتدار و دیگر مولفه‌های تاثیرگذار CERT پرداخته شده است.

۱-۳- مدل‌های بکارگیری CERT

الف- گروه امنیتی (بکارگیری کارکنان موجود فن‌آوری اطلاعات)

این مدل، یک CERT 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 حل و فصل می‌گردد. از مدیران سیستم، شبکه و امنیت که این کار را انجام می‌دهند، به عنوان «گروه

امنیتی» نام برده می‌شود. مشکلی این مدل نبود راهی برای تضمین پاسخ گویی صحیح و منسجم در کل سازمان است (کیلکرس و همکاران، ۲۰۱۱).

ب– CERT توزیع شده داخلی

در چنین الگویی که CERT " پراکنده " نیز نامیده می‌شود، گروه ترکیبی از کارکنانی به مدیریت مرکزی CERT 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 حل و فصل حادثه‌ها، ۲) ایجاد روش ارتباطی با کل تشکیلات درباره تهدیدات امنیتی و راهبرد پاسخ‌گویی و ۳) اعضای گروه و یک مدیرCERT معین که به صورت اختصاصی برای وظایف رفع یک حادثه تعیین شده‌اند از الگوی گروه امنیتی متفاوت است (آلبرت، دروفی، کیلکرنس، رافائل، ۲۰۱۰، توصیف پردازشی مدیریت رایانه‌ای)

ج– CERT متمرکز داخلی

مدل CERT متمرکز داخلی، یکCERT اختصاصی است که در سازمان متمرکز شده است و مسئولیت کامل گزارش‌دهی، تحلیل و پاسخگویی به همه حادثه‌ها را بر عهده دارد. در این حالت معمولاً اعضای تیم کل وقت خود را به کارهای مربوط به CERT و رفع حادثه‌ها اختصاص می‌دهند. این نوعCERT دارای مدیری است که به مدیریت رده بالای سازمان گزارش می‌دهد. تمامی منابع CERT در یک نقطه متمرکز شده‌اند. این مدل در با نام " CERT متمرکز" نیز شناخته می‌شود(کاساکواساکی و همکاران، ۲۰۱۰).

د– CERT توزیع شده و متمرکز (ترکیبی یا هیبریدی)

در این مدل، یک CERT متمرکز اختصاصی به وجود می‌آید که اعضای آن در سازمان، در موقعیت‌های جغرافیایی و شعب مختلف توزیع شده‌اند. 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 Artifacts را برای اعضای توزیع شده تیم و سایر بخش‌های سازمان انجام می‌دهد. اعضای پراکنده تیم در هر سایت راهبردها را پیاده سازی می‌کنند و در حوزه‌های مسئولیت خود، مهارت و دانش خود را در اختیار دیگران قرار می‌دهند. این مدل با عنوان CERT ترکیبی شناخته می‌شود (همان).

ه- CERT هماهنگ کننده

در این مدل تمرکز اصلی CERT 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 پاسخ گویی 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 آسیب پذیری، بنگاه‌های پایاپای سازی ابزارهای امنیتی[1]، یا خدمات اعلان خطر و مشاوره باشد(سایت اینترنتی CERT ژاپن، ۲۰۱۱).

۲-۳- اقتدار

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

۱: اقتدار کامل

یعنی این که CERT 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، هنگامی که یک حادثه امنیتی اتفاق می‌افتد CERT می‌تواند در صورت لزوم، بدون آنکه منتظر اجازه مدیران رده بالا بماند تصمیم گیری کند. برای مثال یک ERT، با اقتدار کامل می‌تواند در صورت بروز یک حمله، به مدیران سیستم‌ها اعلام کند تا آن‌ها را از شبکه قطع کنند (سایت اینترنتی مرجع CERT. (۲۰۱۱) (CERT.org/ CSIRTServices

۲: اقتدار مشارکتی

یعنی این که CERT می‌تواند در فرآیند تصمیم‌گیری در خصوص اقدامات لازم برای مراکز تحت پوشش مشارکت نماید. در این حالت CERT قادر است بر نتیجه تصمیم‌گیری تأثیر بگذارد اما تنها بخشی از فرآیند تصمیم‌گیری است و نه تصمیم گیرنده. در چنین شرایطی CERT می‌تواند به مدیران شبکه توصیه کند که هنگام بروز حمله، از شبکه قطع شوند و اقدامات لازم (با توجه به توصیه‌های ارائه شده) را با سایر اعضای مراکز تحت پوشش در میان بگذارند (همان).

[1] - clearing houses for security tools

۳: فقدان اقتدار

یعنی این که CERT تنها می‌تواند به عنوان یک مشاور(البته بسیار قوی) برای یک سازمان عمل کند.CERT نمی‌تواند به تنهایی هیچ تصمیمی بگیرد یا اقدامی انجام دهد. این تیم می‌تواند توصیه کند که سیستم‌ها هنگام بروز حمله قطع شوند اما هیچ‌گونه تأثیری در تصمیم گیری نهایی نخواهد داشت. با این حال می‌توان در صورت عدم تبعیت مراکز از توصیه‌هایCERT 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 CERT تأثیر مثبتی داشته باشد (همان).

۳–۳: انواع خدمات قابل ارائه CERT

در حقیقت استانداردی از مجموعه کارها و سرویس‌هایی که یک گروه 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 گروه پاسخگویی به حوادث رایانه‌ای ارائه می‌شود را می‌توان در سه گروه رده‌بندی کرد: سرویس‌های واکنشی، سرویس‌های پیشگیرانه و سرویس‌های مدیریت کیفیت امنیت(جورجیا کیلکرنس، ۲۰۰۴).

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 منتشر شده‌اند، آسیب پذیری رایانه‌ای یا موردی که توسط کشف یک سیستم ردیابی اختلال یا ثبت ورود شناسایی شده است، خدمات واکنشی وظایف پایه یک CERT هستند(همان).

ب:خدمات غیر انفعالی(پیشگیرانه)

این خدمات، راهنمایی‌ها و اطلاعات لازم برای کمک به آماده سازی، حفاظت و ایمن سازی سیستم‌های تحت پوشش را فراهم می‌کنند. ارائه چنین خدماتی، به کاهش تعداد حوادث آتی می انجامد (همان).

ج:خدمات مدیریت کیفیت امنیت

این خدمات موجب تکمیل خدمات از قبل تعیین شده است که مستقل از رسیدگی به حوادث هستند و به صورت سنتی توسط دیگر بخش‌های سازمان همانند بخش‌های فناوری اطلاعات، بازرسی، یا آموزشی ارائه می‌شوند(همان). این خدمات در جدول(۱) فهرست شده است.

جدول(۱): خدمات مدیریت کیفیت امنیت(جورجیا کیلکرنس، ۲۰۰۴، مراحل ایجاد CERTملی).

خدمات انفعالی(واکنشی)	خدمات غیر انفعالی(پیش‌گیرانه)	خدمات مدیریت کیفیت امنیت
اخطارها و اعلام خطرها	اطلاع رسانی	تحلیل ریسک
رسیدگی به حادثه	نظارت بر فناوری	برنامه‌ریزی تداوم کسب و کار و بازیابی از فجایع
تحلیل حادثه	ممیزی یا ارزیابی امنیتی	مشاوره امنیتی
پاسخ‌گویی به حادثه در محل	پیکربندی و نگهداری ابزارها، برنامه‌ها و زیرساخت‌های امنیتی	آگاه سازی
پشتیبانی از پاسخ‌گویی به حادثه	توسعه ابزارهای امنیتی	تربیت/آموزش
هماهنگی پاسخ‌گویی به حادثه	خدمات ردیابی اختلال	ارزیابی یا صدور گواهی برای محصول
رسیدگی به آسیب‌پذیری	انتشار اطلاعات امنیتی	
تحلیل آسیب‌پذیری		
پاسخ‌گویی به آسیب‌پذیری		
هماهنگی پاسخ‌گویی به آسیب-پذیری		
بررسی Artifact		
تحلیل Artifact		
پاسخ‌گویی به Artifact		
هماهنگی پاسخ‌گویی Artifact		

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 به طور وسیع خود را نشان دهند یا مورد بهره‌برداری قرار گیرند، قابل حل خواهند بود(جورجیا کیلکرنس، ۲۰۰۴).

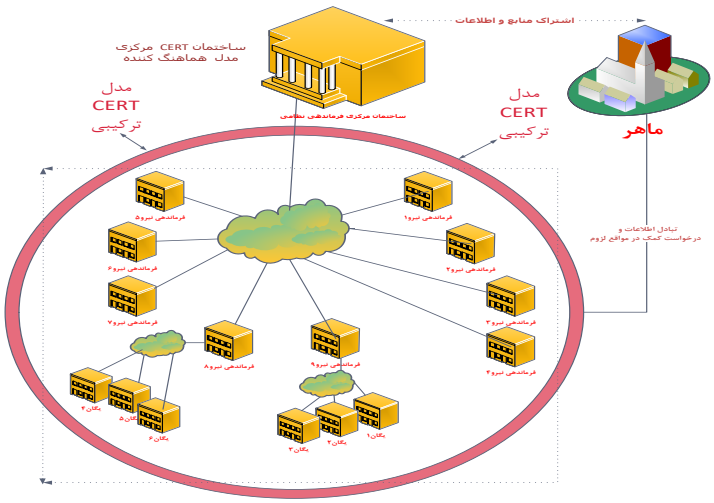
در ادامه **ساختار** CERT مورد نیاز مراکز نظامی که شامل مأموریت‌ها، اهداف و مقاصد، محدوده عملکرد، نوع و سطح سرویس‌ها، میزان اختیارات تیم، جایگاه آن در سازمان، مدل سازمانی CERT ارایه می‌شود. در این روش راهکارها بر مبنای مطالعات صورت گرفته و استفاده از نظرات خبرگان و در قالب پرسش‌نامه انجام و مبنای تحقیق قرار گرفته است. در طرح کلان اولیه نوع مدل سازمانی، نیروی انسانی، اقتدار CERT، سازمان‌های سرویس‌گیرنده و سرویس‌های مورد نیاز CERT مراکز نظامی مشخص شده‌اند.

۴: پیشنهاد مدل سازمانی، چارت سازمانی، بخش‌ها و سرویس‌های قابل ارایه CERT مراکز نظامی(تجزیه و تحلیل نتایج صورت گرفته)

پس از نظرسنجی از خبرگان نظامی در حوزه سایبری و تنظیم پرسش‌نامه‌ها و تحلیل نتایج آماری، مدل سازمانی، چارت سازمانی و سرویس‌هایی که CERT نظامی پیشنهاد می‌گردد:

۴–۱: مدل پیشنهادی سازمانی CERT

مدل سازمانی که باید برای مراکز نظامی در نظر گرفته شود با توجه به محدوده جغرافیایی و پراکندگی سازمان و قرار گرفتن سرویس‌گرها و تجهیزات فناوری اطلاعات لحاظ می‌شوند. مراکز نظامی 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، به صورت مرکزی مدیریت می‌شوند.



شکل ۱: نمایش لایه‌های CERT مراکز نظامی و ارتباط آن‌ها با مرکز ماهر

با توجه به پراکندگی و نیاز به داشتن یکپارچگی در مأموریت 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 توزیع پذیر) را می‌توان برای مراکز نظامی و زیرمجموعه‌های تابعه آن مطابق با شکل(۱) در نظر گرفت. هر چند که مدل متمرکز نیز تا حدی می‌توانست برای مراکز نظامی 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 نظامی مطابقت دارد. فرماندهی نظامی با توجه به تمرکز مدیریت، به عنوان CERT هماهنگ‌کننده برای برقراری ارتباط بین CERT های مراکز عمده نظامی و دیگر زیرمجموعه‌ها پیشنهاد می‌گردد. نقاط قوت و ضعف هر یک از مدل‌ها به تفکیک در جدول (۲) آمده است؛ همچنین ویژگی‌های عمده مدل ترکیبی در مراکز نظامی عبارتند از :

- تشکیل بخش متمرکز CERT به صورت هسته‌ای پایدار از افراد متخصص،
- توزیع تعدادی از کارمندان موجود در موقعیت‌های استراتژیک سازمان و دیگر زیرمجموعه‌ها،
- جمع آوری، ترکیب و پیگیری تمامی گزارش‌ها توسط اعضای تیم مرکزی،

- تحلیل مناسب و کارا و تدوین راهبردهای مهار رخدادها توسط تیم مرکزی،
- پیاده سازی راهبردهای تدوین شده در هسته مرکزی، توسط اعضای پراکنده تیم،
- پاسخ‌گویی سریع‌تر به رخدادها توسط اعضای توزیع شده تیم در سطح مراکز نظامی،
- انتقال مهارت و دانش به حوزه‌های مسئولیت توسط اعضای پراکنده تیم،

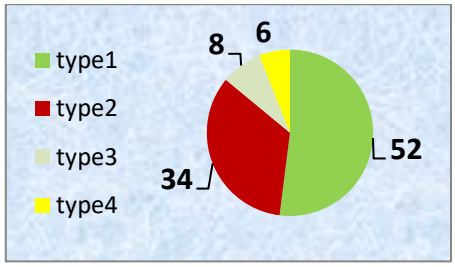
جدول۲: نقاط قوت و ضعف مدل‌های CERT

	گروه امنیتی	توزیع شده داخلی	متمرکز داخلی	توزیع شده و متمرکز داخلی	هماهنگ کننده
نقاط قوت	هیچ نقطه قوتی به دلیل نبود حل و فصلی مشاهده نمی شود	تمرکز در مسوولیت یکپارچگی در ماموریت داشتن پایگاه داده متمرکز داشتن دیدگاه جامع قابلیت نیروهای محلی	داشتن کارکنان متمرکز و اختصاصی و آموزش دیده شناسایی حمله های هدفدار داشتن پایگاه داده قوی پشتیبانی آموزشی قوی رده ها سهولت در حفظ تیم	داشتن نیروهای متمرکز و توزیع شده داشتن پایگاه قوی داده یکپارچگی در ماموریت مسولیت متمرکز و تلفیقی پشتیبانی آموزشی قوی رده ها سهولت در پیاده سازی دستورالعملها	دارای کارکنان اختصاصی و کارآزموده دارای یک واحد قوی گزارش دهی دارای واحدی متمرکز برای تحلیل اطلاعات دارای یک پایگاه داده قوی وجود تریاژ در خارج سازمان پشتیبانی قوی آموزشی رده ها
نقاط ضعف	نبود ضمانت اجرایی عدم مشارکت گروه ها هزینه کمتر و لی آسیب بیشتر عدم هماهنگی پرسنل دشواری در تعیین مسول رسیدگی	کمبود نیروی متخصص نبود فیدبک برای صحت انجام کارها عدم مقیاس گذاری در مناطق بزرگ دشواری در حفظ یکپارچگی امکان تحمیل مسوولیت مازاد نیاز به پشتیبانی مدیریت به روز نگه داشتن اطلاعات افراد	دشواری هماهنگی با سایتهای شعب ایزوله بودن از نظر پرسنل دشواری حفظ پشتوانه مالی دشواری در اطاعت پذیری رده ها امکان کمبود نیرو برای پشتیبانی لازم زمان طولانی برای انجام فرامین به روز نگه داشتن اطلاعات افراد	دشواری در مدیریت و هماهنگی دشواری حفظ منابع مالی نیاز شدید به پشتیبانی مدیریت امکان کمبود منابع انسانی و مالی برای پشتیبانی لازم نیاز به خرید یک سیستم ردیابی قوی امکان ایزوله بنظر رسیدن اعضای متمرکز نیاز به استخدام نیرو و تجهیزات	دشواری هماهنگی با رده ها ایزوله بودن از نظر بقیه امکان پشتیبانی مالی رده ها پیچیدگی تعیین تعداد کارکنان دشواری پوششی مدیریت ثابت نبودن کارشناسان رده ها عدم ارسال بموقع رده ها نبود فیدبک از اجرای اخطارها زمانبری اجرای فرامین نیاز به خریداری سیستم ردیابی قوی جلب اعتماد رده های تحت پوشش به روز نگه داشتن افراد

۲-۴: تعیین فرآیند گزارش گیری (تریاژ)

برای دریافت گزارش و فرآیند دسته‌بندی و ارسال گزارشات بر حسب اولویت چهار نوع دسته بندی برای آن وجود دارد که در روش اول تمامی گزارشات به مرکز وارد شده و پس از دسته‌بندی و اولویت‌گذاری به تیم توزیع شده واگذار می‌شود. در روش دوم گزارشات به سایت‌های توزیع شده می‌روند و گزارش‌گیری اولیه در آنجا انجام می‌شود و در صورت عدم امکان رسیدگی به آن‌ها در قسمت‌های توزیع شده 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 توزیع شده، به افراد مناسبی از آن‌ها محول می‌کند و در روش چهارم از روش FIFO[1] برای اولویت‌گذاری گزارش‌های حوادث و درخواست‌های CERT استفاده می‌شود که در نظر سنجی‌های صورت گرفته روش اول ۵۲٪ و روش دوم ۳۴٪، روش سوم ۸٪ و روش چهارم ۶٪ انتخاب شد. شکل شماره (۲) نظرسنجی تریاژ CERT نظامی نشان داده شده است.

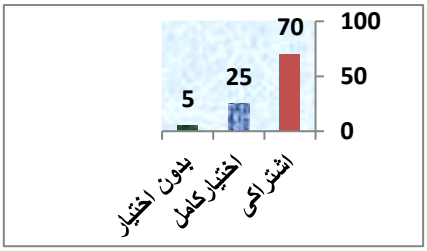


شکل ۲: نظر سنجی تریاژ CERT

۳-۴: تعیین میزان اختیارات CERT مراکز نظامی

یکی دیگر از مواردی که باید به آن توجه نمود میزان اختیاراتی است که تیم CERT نظامی دارد. در این تصمیم‌گیری باید اختیار CERT را از بین سه دسته اختیار کامل، اختیار مشارکتی و فقدان اختیار انتخاب نمود. در سازمان‌های نظامی با توجه به این‌که تمامی دستورات و فرامین باید فرآیند خاصی را طی نمایند، لذا داشتن اختیار کامل برای CERT نظامی ممکن نیست؛ همچنین در صورت نداشتن اختیار، CERT عملاً در مجموعه فقط به سرویس هشداردهی و اعلان پیام‌های امنیتی محدود خواهد شد؛ لذا اگر تیم ترکیبی، اختیار کاملی در تحلیل فعالیت‌ها داشته باشد و برای پاسخ‌گویی به حادثه‌ها دارای اختیار اشتراکی باشد، عملکرد بهتری خواهد داشت. بنابراین در CERT نظامی 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 به انجام 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 (۳) نظرسنجی میزان اختیارات CERT نظامی نشان داده شده است.

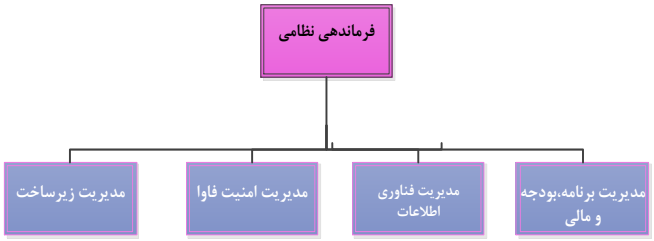
[1] -First In First Out



شکل۳: نظر سنجی در مورد میزان اختیار و اقتدار CERT

۴–۴: مشارکت‌کنندگان در راه اندازی CERT نظامی

با توجه به نظر خبرگان، بخش‌های که در راه‌اندازی CERT مراکز نظامی نقش آفرینی می‌کنند به صورت شکل(۴) می‌باشند:



شکل۴: بخش‌های مرتبط در ایجاد CERT ترکیبی نظامی

۵–۴: تعیین سرویس‌های مورد نیاز

برای راه‌اندازی یک تیم CERT ترکیبی، خدماتی که CERT ترکیبی باید ارائه دهد به دو قسمت خدمات اصلی و خدمات اضافی تقسیم می‌شوند؛ هر چند که پیشنهاد می‌شود در مراحل ابتدایی و آغازین، سرویس‌های اضافی راه‌اندازی نشود ولی در صورت داشتن شرایط لازم بلامانع است. این سرویس‌ها در جدول(۳) ارایه گردیده است.

جدول۳:سرویس‌های ارائه شده CERT رده‌ها (مدل ترکیبی)

ردیف	سرویس‌های اصلی	CERT@MILITARY
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	√
	سرویس‌های اضافی	
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 زیر ساخت‌های امنیتی	*

۶	**توسعه ابزارهای امنیتی**	*

۶-۴: بخش‌های مورد نیاز CERT نظامی

سرویس‌های مورد نیاز اعم از اصلی و اضافی بخش‌های تعریف شده باید سرویس‌های مرتبط با مدل ارایه شده را پوشش دهند؛ بخش‌های مورد نیاز برای CERT نظامی به ۴ بخش عمده تقسیم می‌شود:

۱: بخش اجرایی و پاسخگویی

این بخش خدمات مربوط به سرویس‌های زیر را انجام می‌دهد:

- پشتیبانی پاسخ‌گویی به رخداد،
- هماهنگی در پاسخ‌گویی به رخداد،
- هماهنگی در پاسخ‌گویی به حفره‌های امنیتی و آثار باقی‌مانده،
- پاسخ‌گویی به رخداد در محل.

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:

- هشدارها و اخطارها،
- تحلیل رخداد،
- سرویس‌های تشخیص نفوذ،
- تحلیل حفره‌های امنیتی و آثار باقی‌مانده از حمله،
- ممیزی یا ارزیابی امنیتی.

۳: بخش آموزش و تولید محتوا

در این بخش مدل CERT 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:

- اعلان‌ها،
- پایش فناوری،
- انتشار اطلاعات مرتبط با امنیت.

۴: بخش پشتیبانی

سرویس‌های زیر مربوط به بخش پشتیبانی می‌باشد:

- تنظیم، پیکر بندی و نگهداری ابزارها، نرم افزارها و زیر ساخت های امنیتی،
- توسعه ابزارهای امنیتی.

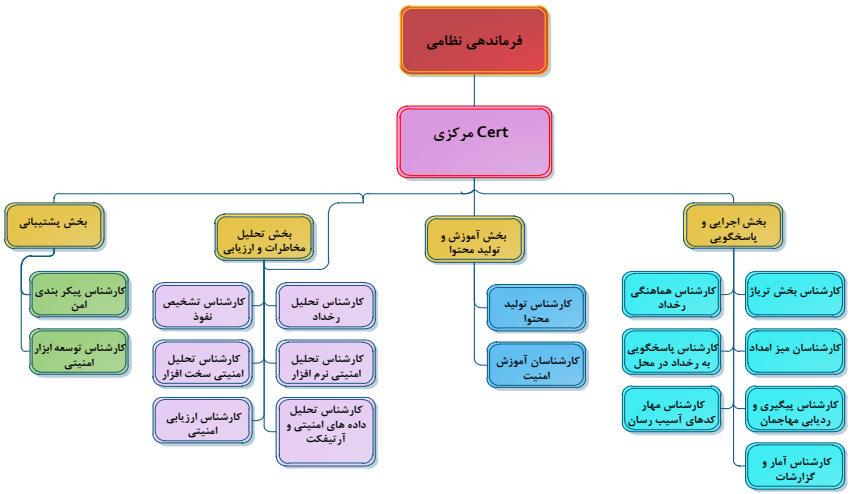
در جدول (۴) بخش‌ها و سرویس‌های قابل ارایه در CERT نظامی ارایه گردیده است.

جدول۴: بخش‌ها و سرویس‌های ارائه شده در CERT ترکیبی

	بخش های cert	سرویس ها
۱	بخش اجرایی و پاسخگویی	• پشتیبانی پاسخگویی به رخداد • هماهنگی در پاسخ گویی به رخداد • هماهنگی در پاسخگویی به حفره های امنیتی و آثار باقیمانده • پاسخگویی به رخداد در محل
۲	بخش تحلیل مخاطرات و ارزیابی	• هشدارها و اخطارها • تحلیل رخداد • سرویس های تشخیص نفوذ • تحلیل حفره های امنیتی و آثار باقیمانده از حمله • ممیزی یا ارزیابی امنیتی
۳	بخش آموزش و تولید محتوا	• اعلان ها • پایش فناوری • انتشار اطلاعات مرتبط با امنیت
۴	بخش پشتیبانی	• تنظیم، پیکر بندی و نگهداری ابزارها، نرم افزارها و زیر ساخت های امنیتی • توسعه ابزارهای امنیتی

۴-۷: جایگاه و چارت سازمانی

CERT بنا به موقعیت می‌تواند جایگاه مختلفی داشته باشد، CERT از نظر جایگاه ساختمانی می‌تواند در موقعیت‌های متفاوتی قرار گیرد. می‌تواند درون بخش‌های فناوری اطلاعات یا بخش امنیت و حتی در بخش زیر ساخت به عنوان یک واحد باشد یا اینکه می‌تواند به عنوان یک بخش مستقل زیر نظر مستقیم فرماندهی قرار گیرد و این بسته به اقتداری است که در سازمان برای آن تعریف می‌شود. به عنوان مثال CERT ایالات متحده یا همان Us-CERT با توجه به نفوذ خود می‌تواند ارتش را به عکس العمل‌هایی وادار کند. در CERT نظامی با توجه به گستردگی و اقتدار مشارکتی بهتر است که بخشی مستقل زیر نظر فرماندهی بوده و اجزاء تشکیل یافته یا همان چارت سازمانی به صورت پیشنهادی شکل(۵) بر اساس تعداد مورد نیاز برای مدل ترکیبی CERT ارایه می‌نماید.



شکل ۵: جایگاه و چارت پیشنهادی CERT

۵– نتیجه‌گیری

در این مقاله پس از تبیین مفاهیم CERT، مدل‌ها، سرویس‌ها و خدمات CERT و دیگر مولفه‌ها و موارد اثرگذار در CERT مورد بررسی قرار گردید؛ سپس در پیشینه تحقیق، دو نمونه از CERT های مهم دنیا(آمریکا و کره جنوبی) مورد بررسی اجمالی قرار گرفت و اهداف آنها از به‌کارگیری CERT بیان گردید؛ در نهایت، پس از اجماع نظر خبرگان نظامی در حوزه سایبری و تحلیل آماری، مدل مفهومی CERT نظامی، سرویس‌ها و جایگاه و دیگر موارد مهم CERT نظامی پیشنهاد گردید؛ در پیشینه تحقیق با توجه به ضرورت 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 ساز و کار مناسب، امنیت شبکه‌ها و زیرساخت سایبری خود را ارتقاء دهند؛ تمامی موارد ذکر شده، نتایج بررسی یک تحقیق علمی است، اما نکته مهمی که در اکثر مقالات به‌صورت مغفول باقی می‌ماند، جلب نظر مدیران و مسئولان راهبردی و تصمیم‌گیر است؛ و لذا امید است با مطالعه این تحقیق، مدیران و مسئولان تصمیم‌گیر ج.ا.ا در سطح راهبردی به ضرورت و اهمیت راه‌اندازی CERT بالاخص در مراکز نظامی پی برده و آن را از اولویت‌های اصلی سازمان قرار دهند تا به یاری خدا و پیرو فرمایشات فرماندهی معظم کل قوا امام خامنه‌ای (مدظله‌العالی)، شاهد پویایی و حضور مقتدرانه جمهوری اسلامی ایران در فضای سایبری باشیم.

مراجع

الف– فارسی

۱- کشاورز رضا، ارایه الگوی استقرار CERT مراکز نظامی، مجله علمی پژوهش های حفاظتی ۱۳۹۲.

۲- طیرانی احسان، مدیریت رخدادهای امنیت رایانه ای و تشکیل تیم های CERT سازمانی، آپای مشهد، ۱۳۹۵.

۳-رشتی سیدمحمد رضا، رشتی زهرا، سیفی مهدی،۱۳۹۲، راهنمای ایجاد یک تیم پاسخ‌گویی به رخدادهای امنیتی رایانه‌ایCSIRT.

ب– انگلیسی

1. [Online]. http://www.cyberpolice.irnews/home

2. Penedo, David. (Aug 2006). "Technical Infrastructure of a CSIRT". Cote d'Azur: *Internet Surveillance and Protection, ICISP '06. International Conference,* : 27 – 27

3. J. West-Brown, Moira. Stikvoort, Don. Kossakowski, Klaus-Peter. Audrey. Killcrece, Georgia. Ruefle, Robin. Zajicek, Mark. (April 2003). "Handbook for Computer Security Incident Response Teams (CSIRTs)". CMU/SEI-2003-HB-002. U.S: Software Engineering Institute, Carnegie Mellon University.
[Online]. <http://www.sei.cmu.edu/reports/03hb002.pdf>. [Mar 2010]

4. National Cyber Incident Response Plan ،EMERGENCY RESPONSE FRAMEWOR.۲۰۱۷ .

5. Scarfone, Karen. Grance, Tim and Masone, Kell. (March 2008). "Computer Security Incident Handling Guide". NIST SP 800-61. U.S: Department of Commerce, National Institute of Standards and Technology.
[Online]. < http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf>.

6. Albert,C , Dorofee,A ,Killcrece, G, Ruefle, R,Zajicek, (2010), M. Defining Incident Management Processes for CSIRTS:A Work in Progress. Available at www.CERT.org/archive/pdf/04tr015.pdf

7. Killcrece, G.,Kossakowski ,K., Ruefle ,R.,Zajicek ,M., State of the Practice of Computer Incident Response Teams (CSIRTs). p. 291.Available at www.CERT.org/archive/pdf/03tr001.pdf

8. Creating A CSIRT ,Keisuke KAMATA, JPCERT/Coordination Center, Japan
9. "CSIRT Services", <http://www.CERT.org/ CSIRTs/services.html>.
10 Team, CERT® Coordination Center, Networked Systems Survivability Program, Software Engineering Institute, Carnegie Mellon University, Pittsburgh PA 15213-3890, USA, August 2004.
11. "Clearinghouse for Incident Handling Tools", © 2005-2011 by the European Network and information Security Agency (ENISA), http://www.enisa.europa.eu/act/CERT/support/chiht.