به نام خدا

پدافند غیر عامل باید همچون شعله‌ای بلند شود.

مقام معظم رهبری

پدافند غیرعامل– تیم پاسخگویی به رویدادهای امنیتی کامپیوتر (CERT)

فهرست:

مقدمه

تأمین امنیت اطلاعات سازمان ها در محیط امروزی که از شبکه های به هم پیوسته تشکیل شده، کاری مشکل است و با ورود هر محصول الکترونیکی و هر ابزار نفوذ جدید این کار صعب، سخت تر نیز می شود. اکثر سازمان ها متوجه شده اند که یک راهکار امنیتی واحد برای تأمین امنیت سیستم ها وجود ندارد بلکه باید از استراتژی امنیتی چند لایه بهره گرفت. یکی از لایه هایی که بیشتر سازمان ها در استراتژی امنیتی خود در نظر می گیرند، ایجاد یک تیم برای پاسخگویی به رویدادهای امنیتی کامپیوتر است که اختصاراً CSIRT نامیده می شود. البته این تیم نام های دیگری مانند تیم پاسخگویی به فوریت های کامپیوتری (CERT) نیز دارد اما کارکرد مشابهی دارند که در ادامه به آن خواهیم پرداخت.

با وجود آنکه تیم های CSIRT از سال ۱۹۸۸ پای به عرصه وجود گذاشته اند اما در واقع توسعه CSIRT و موضوع پاسخگویی به رویداد در دوران ابتدایی فعالیت خود به سر می برد، به همین دلیل است که هنوز به یک موضوع استاندارد شده عملیاتی بدل نشده است اما به سرعت به این سمت در حال حرکت است. بسیاری از سازمان ها سعی دارند تا به متدولوژی ها، پردازه ها و ساختار سازمانی پاسخگویی به رویدادهای امنیتی رسمیت بخشند.

فصل ۱ - تعریف CSIRT

CSIRT یک سازمان خدماتی است که مسئول دریافت، مرور و پاسخگویی به گزارشات ارسالی و فعالیتهای مربوط به مشکلات و رویدادهای کامپیوتری است. سرویس های این سازمان معمولاً برای محدوده مشخص تعریف می شود که می تواند یک شرکت، اداره دولتی، سازمان آموزشی یا یک منطقه یا کشور باشد.

براساس تعریف ارائه شده در پروژه CIFAC[۱]، یک رویداد کامپیوتری عبارتست از هر عمل یا رخداد عمدی یا سهوی که برروی منابع اطلاعات رخ دهد یا به گونه ای شامل آنها شود و بطور بالقوه باعث بی ثبات کردن، مختل کردن و یا تخریب منابع، سیاست ها، سرویس ها یا داده های اشخاص یا اجتماع شود.

بخشی از فعالیت های یک CSIRT را می توان با واحد آتش نشانی مقایسه نمود. زمانی که یک آتش سوزی رخ می دهد، واحد آتش نشانی وارد عمل شده، به محل حریق می روند و خسارات را برآورد می کنند، پس از بررسی الگوی حریق درباره شیوه برخورد با آن تصمیم گیری کرده و در نهایت با توجه به بررسی ها آتش را مهار می کنند. این روال کاملاً مشابه سرویس های واکنشی (Reactive) در یک CSIRT است.

---

[۱] Computer Incident Factor Analysis and Categorization

یک CSIRT درخواست های کمک و گزارشات تهدید، حمله، اسکن، استفاده نامناسب از منابع یا دسترسی غیرمجاز به داده ها و اطلاعات را دریافت می نماید. سپس گزارش را تحلیل می نماید تا تعیین کند که چه اتفاقی در حال انجام است و تصمیم بگیرد که چه عکس العملی مناسب است. ارائه خدماتی نظیر آموزش، آگاهی و اطلاع رسانی امنیتی، مشاوره امنیتی، نگهداری پیکربندی و ارائه مستندات فنی و توصیه های امنیتی سیستم های کامپیوتری نیز از دیگر خدمات یک CSIRT می باشد.

اهداف یک CSIRT بر اساس اهداف مجموعه تحت پوشش آن تعریف می شود. محافظت از دارایی های مهم، کلید موفقیت یک سازمان و CSIRT آن است. هدف اصلی یک CSIRT کاهش و کنترل خسارت، فراهم آوردن پاسخ و ترمیم مناسب و اندیشیدن راهکارهایی برای جلوگیری از رویداد بعدی است. CSIRT برای ایفای این نقش، اطلاعات حوادث، نقاط ضعف امنیتی و حفره های امنیتی سیستم و نرم افزار را در زیرساخت سازمانی جمع آوری می نماید.

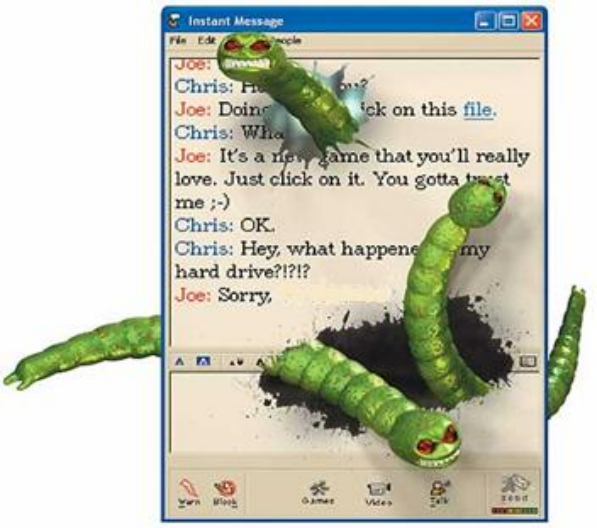
ساختار، وظایف و اسامی CSIRT ها با یکدیگر متفاوت می باشد. هر CSIRT با توجه به تفاوت های موجود در اهداف، مأموریت ها و حوزه کاری خود در تعاریف و ارائه سرویس های

خود با دیگران تفاوت دارد. جدول زیر اسامی متفاوت با معنای مشابه را برای CSIRT نشان می دهد. با وجود آنکه اسامی متفاوت هستند، تمامی این تیم ها به پاسخگویی به رویدادهای امنیتی می پردازند.

اسامی متفاوت با معنای مشابه برای CSIRT		
CSIRT	Computer Security Incident Response Team	تیم پاسخگویی به رویداد امنیتی کامپیوتری
CSIRC	Computer Security Incident Response Capability	توانایی پاسخگویی به رویداد امنیتی کامپیوتری
CIRC	Computer Incident Response Capability	توانایی پاسخگویی به رویداد کامپیوتری
CIRT	Computer Incident Response Team	تیم پاسخگویی به رویداد کامپیوتری
IHT	Incident Handling Team	تیم مدیریت رویداد
IRC	Incident Response Cnter or Incident Response Capability	مرکز پاسخگویی به رویداد یا توانایی پاسخگویی به رویداد
IRT	Incident Response Team	تیم پاسخگویی به رویداد
SERT	Security Emergency Response Team	تیم پاسخگویی به فوریت های امنیتی
CERT	Computer Emergency Response Team	تیم پاسخگویی به فوریت های کامپیوتری
SIRT	Security Incident Response Team	تیم پاسخگویی به رویداد امنیتی

فصل ۲ - تاریخچه و توسعه توانایی های CSIRT

انگیزه اصلی برای ایجاد اولین CSIRT، انتشار کرم موریس در سال ۱۹۸۸ بود. این کرم که توسط یک دانشجوی ۲۳ ساله نوشته شده بود، خود را با استفاده از حفره های امنیتی مختلف از یک کامپیوتر به کامپیوتر دیگر منتشر می کرد.



بنابر مستندات تاریخی در آن زمان حدود ۶۰۰۰۰ تا ۸۰۰۰۰ سیستم بر روی شبکه اینترنت وجود داشت (این شبکه آرپانت نام داشت) و ۱۰ درصد آن دستگاه ها توسط این کرم آلوده شدند. مشکل اصلی آن بود که بسیاری از سیستم هایی که آلوده شده بودند، رله ایمیل و سرورهای زیرساخت اصلی اینترنت بودند. بسیاری از سایت ها سیستم های خود را از شبکه خارج کردند تا

آلوده نشوند. نتیجه حمله این کرم از کار افتادن بسیاری از مسیرهای ارتباطی اینترنت بود.

پس از آنکه حمله کرم مهار شد، مرکز ملی امنیت کامپیوتر آمریکا (بخشی از آژانس امنیت ملی) جلساتی را برگزار نمود تا درباره جلوگیری و پاسخگویی به حوادث مشابه در آینده تصمیم گیری نماید. در روز ۸ نوامبر ۱۹۸۸ جلسه کالبدشکافی این واقعه توسط آژانس پروژه های تحقیقات پیشرفته دفاعی (DARPA) تشکیل شد و به بحث و بررسی درسهایی که از حمله این کرم آموخته شده بود، پرداخت.

در این جلسه مشاهدات زیر بدست آمد:

- در این بررسی مشخص شد که بسیاری از سایتها در تحلیل فعالیت کرم به کار تکراری و موازی مشغول بوده اند در حالیکه اگر همکاری و هماهنگی لازم صورت پذیرفته بود، زمان به شکل مفیدتری استفاده شده بود. همچنین مشخص شد که اگر تحلیل گران تمامی سایت های درگیر با یکدیگر ارتباط داشتند و به مقایسه نتایج حاصله می پرداختند؛ تحلیل کامل زود هنگامی به دست می آمد و در نتیجه فعالیت کرم سریعتر مهار می شد و فاز ترمیم و حفاظت نیز زودتر آغاز می شد.

- ابزارها و روش های اصلاحی حاصله از تحلیل می توانست از آلودگی های بیشتر جلوگیری کند. از آنجایی که وسایل ارتباطی در دسترس نبود، توزیع این ابزارها و روش ها برای تمامی کسانی که به این اطلاعات نیاز داشتند امکانپذیر نبود و بسیاری از سایتها به موقع به این اطلاعات دسترسی پیدا نکردند.
- از آنجاکه سازمانهای تحت تأثیر به فایلهای پشتیبان موجود اعتماد کرده بودند، ترمیم خرابی پر دردسر اما سرراست بود. البته بدلیل آنکه تمامی ابزارها و روش های اصلاحی برای همه توزیع نشده بود، بسیاری از سایتها پس از ترمیم، مجدداً آلوده شدند.

در این جلسه مشخص شد که مهم ترین مشکل در زمان پاسخگویی عدم وجود مکانیزم های ارتباطی سالم بوده است. بسیاری از سایتها به دلیل آلودگی از شبکه قطع شده بودند تا به ترمیم سیستم های خود بپردازند. سرویس ایمیل نیز به دلیل آلودگی سرورها و رله کننده های مربوطه از کار افتاده بود لذا راه سریع و مناسبی برای اطلاع رسانی جهت مقابله و پاسخگویی به حمله کرم وجود نداشت. در مجموع روش مشخصی برای مدیریت چنین حمله ای علیه امنیت کامپیوتر وجود نداشت.

با تشخیص این مشکل، DARPA اعلام نمود قصد دارد برای تأسیس یک مرکز هماهنگی رویداد امنیتی در اینترنت

سرمایه گذاری کند. این مرکز تیم پاسخگویی به فوریت های کامپیوتری (CERT) نامیده شد. سرانجام CERT به عنوان یک نشان خدماتی دانشگاه Carnegie Mellon شناخته شد و نام مرکز به CERT Coordination Center (CERT/CC) یا مرکز هماهنگی CERT تغییر نام داد. CERT/CC در دسامبر ۱۹۸۸ آغاز بکار کرد. این مرکز در ابتدا ۴ نفر متخصص فنی و یک مدیر داشت.

نتایج حاصله از بررسی های DARPA نشان می داد که یک تیم، به تنهایی نمی تواند پاسخگوی نیاز باشد. طی سال بعد سازمان های دیگر مانند وزارت انرژی آمریکا، اداره ملی فضا و هوانوردی (NASA) ، موسسه ملی استاندارد و فناوری و نیروهای نظامی آمریکا هر یک تیم خود را مشابه CERT/CC اما با تمرکز بر روی حوزه کاری خود ایجاد نمودند. در آگوست سال ۱۹۸۹ کارگاهی توسط CERT/CC برگزار شد تا علاوه بر بررسی های فعالیت های سال گذشته، به گام های آتی در هماهنگ کردن ارتباط بین تیم ها بپردازد. این نقطه سرآغازی بود بر کنفرانس های سالانه ای که درحال حاضر به عنوان انجمن تیم های امنیتی و پاسخگویی رویداد (FIRST) شناخته می شود.

جدول ذیل تعداد تیم های CSIRT عضو در FIRST را به تفکیک حوزه جغرافیایی و کشور نشان می دهد. اطلاعات این جدول از سایت FIRST در ماه ژوئن ۲۰۰۸ برداشت شده است.

آمریکای لاتین	تعداد	آمریکای شمالی	تعداد	آسیا	تعداد	اروپا	تعداد
آرژانتین	۱	کانادا	۱۰	استرالیا	۳	اتریش	۱
برزیل	۲	آمریکا	۶۲	چین	۳	بلژیک	۲
شیلی	۱			هند	۱	کرواسی	۱
مکزیک	۱			ژاپن	۱۱	دانمارک	۶
پرو	۲			کره جنوبی	۵	اروپا	۱
اروگوئه	۱			قطر	۱	فنلاند	۵
				سنگاپور	۴	فرانسه	۳
				مالزی	۱	آلمان	۱۶
				تایوان	۲	مجارستان	۱
				تایلند	۱	رژیم اشغالگر قدس	۲
				امارات متحده	۱	ایتالیا	۱
						لیتوانی	۱
						هلند	۵
						نروژ	۲
						لهستان	۱
						روسیه	۱
						اسلونی	۱
						اسپانیا	۴
						سوئد	۳
						سوئیس	۴
						انگلیس	۱۸
مجموع	۸	مجموع	۷۲	مجموع	۳۳	مجموع	۷۹

فصل ۳ - انواع CSIRT

برخی از گروه های CSIRT مانند مرکز هماهنگی تیم پاسخگویی فوریت های کامپیوتری ژاپن (JPCERT/CC) به یک کشور سرویس می دهند. برخی دیگر ممکن است یک دانشگاه (مانند آکسفورد) یک سازمان تجاری (مانند بوئینگ یا سان) یا یک دامنه یا محدوده IP (مانند Telia CERTCC) راپشتیبانی نمایند. همچنین شرکت ها و سازمان هایی نیز وجود دارند که سرویس های CSIRT را به مشتریان در برابر دریافت هزینه ارائه می دهند که برای نمونه می توان به خدمات امنیتی مدیریت شده IBM (IBM-MSS) یا تیم پاسخگویی فوریت های کامپیوتری debis (DCERT) اشاره کرد.

در این بخش پنج مدل سازمانی متعارف برای یک CSIRT بطور خلاصه معرفی شده است؛ البته ممکن است برخی سازمان ها به این نتیجه برسند که بین دو مدل قرار دارند و یا اینکه سازمان آنها شامل چندین سطح از اعمال مربوط به CSIRT می باشد و در حقیقت بیش از یک مدل را شامل می شود.

۱. مدل تیم امنیتی

در این مدل، هیچ گروه یا بخشی از سازمان، مسئولیت رسمی برای مدیریت وقایع رخ داده بر عهده ندارد. در حقیقت هیچ تیم CSIRT ایجاد و تأسیس نشده است. پرسنل در دسترس که معمولاً

شامل مدیر سیستم یا مدیر شبکه یا مدیر امنیت می شوند، در سطح محلی یا بخش، مدیریت وقایع امنیتی را به صورت موردی و گاهی به عنوان یکی از وظایف و مسئولیتهایشان انجام می دهند. این تلاش ها برای کنترل و مدیریت وقایع امنیتی در سازمان لزوماً هماهنگ شده و استاندارد نیستند. ممکن است هیچ گروه یا افراد مشخصی برای جمع آوری اطلاعات از سازمان، تشخیص خرابی و شدت فعالیت های خرابکارانه، تحلیل روند کارها، ارائه گزارش به مدیر ارشد یا انجام عملیات ترمیم یا محافظت وجود نداشته باشد.

۲. مدل CSIRT توزیع شده داخلی

در این مدل، سازمان از کارمندان موجودش برای ایجاد یک CSIRT مجازی استفاده می کند که معمولاً مجوز دارند که با وقایع و رخدادهای امنیتی درگیر شوند. یک مدیر تعیین می شود که فعالیت های این تیم توزیع شده را سرپرستی و هماهنگ کند. در سازمان، افراد بر اساس تخصصشان در سیستم عامل های مختلف، تکنولوژیها، و برنامه های کاربردی یا بر اساس موقعیت جغرافیایی آنها و یا مسئولیت های عملی به عنوان بخشی از این تیم توزیع شده تعریف می شوند. اعضای این تیم توزیع شده می توانند وظایف CSIRT را علاوه بر مسئولیتهای معمولشان انجام دهند و یا اینکه اساساً به طور تمام وقت به کار CSIRT تخصیص داده شوند.

۳. مدل CSIRT متمرکز داخلی

این مدل شامل یک تیم اختصاصی است که عمل مدیریت وقایع را برای یک سازمان انجام می دهد. در بسیاری از شرایط اعضای تیم تمامی وقت خود را صرف کار برای CSIRT می کنند. البته این مدل می تواند با استفاده از کارمندان نیمه وقت بصورت چرخشی نیز پیاده سازی شود. یک مدیر برای CSIRT تعیین می شود که به مدیریت ارشد گزارش می دهد. تیم به صورت متمرکز در داخل سازمان واقع شده و در مقابل تمامی فعالیت های مدیریت وقایع در حوزه کاری خود یا کل مجموعه مسئول است.

٤. مدل CSIRT ترکیبی متمرکز و توزیع شده داخلی

این مدل ترکیبی از مدل های CSIRT متمرکز و CSIRT توزیع شده را ارائه می دهد. این مدل استفاده بهینه از کارمندان موجود در موقعیتهای استراتژیک در سازمان را بیشینه می نماید. در واقع با انجام هماهنگی های لازم توسط تیم اختصاصی و از یک نقطه متمرکز، درک بهتر و وسیعتری از حملات امنیتی و فعالیت هایی که روی حوزه کاری در کل مجموعه اثر می گذارند فراهم می شود.

۵. مدل CSIRT هماهنگ کننده

در این مدل CSIRT کنترل وقایع را در گستره وسیعی از سازمان های داخلی و خارجی که می تواند شامل CSIRT های دیگر هم بشود هماهنگ و ممکن می سازد. CSIRT می تواند نهاد هماهنگ کننده ای برای شاخه های فرعی یک شرکت، شاخه های چندگانه یک سازمان نظامی، موسسه های یک شبکه تحقیقاتی و یا برای سازمان های مختلفی که در یک کشور یا ایالت مشخص وجود دارند، باشد. هماهنگ کردن CSIRT ها معمولاً دامنه وسیعتر و حوزه کاری متفاوت تری را در بر دارد.

مجموعه سرویس های ارائه شده و اینکه چگونه این سرویس ها در جهت کمک به سایر سازمان ها در ارتباط با مسائل مدیریت وقایع به کار گرفته می شوند این مدل را یکسان می سازد. اغلب CSIRT های هماهنگ کننده قدرت کنترلی نسبت به اعضای حوزه کاری خود ندارند. کار اصلی آنها این است که وقایع و آسیب پذیری ها را تحلیل کنند و سرویس ها را هماهنگ و ارائه نمایند. آنها می توانند راهبردها و راه حل های بهبود و کم کردن مشکلات را توزیع کنند.

فصل ٤ - ساختار سازمانی CSIRT

منظور از ساختار سازمانی یک CSIRT، نحوه سازماندهی این تیم جهت ارائه خدمات است. در این ساختار مشخص می شود که CSIRT خدمات را برای چه کسانی تأمین می کند و چه اهداف و فعالیت هایی دارد. همچنین در این ساختار جایگاه CSIRT در سازمان مشخص می شود و در نتیجه تعیین می گردد که CSIRT به چه شخص و مدیری پاسخگوست. در نهایت حوزه و میزان اختیار این تیم در مجموعه مشخص می گردد.

حوزه کاری و عملیاتی

در جامعه تیمهای پاسخگویی به رویداد، منظور از حوزه کاری و عملیاتی، افراد یا سازمانهایی هستند که CSIRT به آنها خدمات ارائه می کند. اعضای یک حوزه برخی خصوصیات و ویژگی های مشترک (شبکه، محل، منطقه و ...) دارند و به عنوان کارمند، مشتری، مشترک، ارباب رجوع یا حتی مصرف کننده اطلاعات شناخته می شوند. حوزه کاری، خود می تواند موجودیت های مختلفی باشد. برای مثال دپارتمان های مجزا در یک سازمان، یک دانشگاه، یک شرکت، اداره دولتی یا نظامی، شرکتهای داخلی یا بین المللی، تأمین کنندگان سرویس یا ایالتهای ملی.

محل استقرار CSIRT در یک سازمان

استاندارد مشخص و ثابتی برای محل استقرار CSIRT در سازمان وجود ندارد. در حال حاضر تیم ها در طیف وسیعی از دپارتمان ها قرار دارند، واحد فناوری اطلاعات، واحد امنیت و حتی واحد بازرسی از جمله دپارتمانهایی هستند که CSIRT در آنها مستقر شده است. حتی می توان یک دپارتمان خاص برای تیم CSIRT داشت و آن را درون هیچ واحد دیگری قرار نداد. همچنین مدیریت استاندارد و مشخصی برای دریافت گزارشات CSIRT نیز مشخص نشده است.

- **میزان اختیار CSIRT**

Authority یا میزان اختیار نشان دهنده کنترلی است که تیم بر فعالیت های خود و حوزه عمل خود در رابطه با امنیت کامپیوتر و پاسخگویی رویداد دارد. در واقع میزان اختیار پایه ارتباط بین تیم و سازمان سرویس گیرنده است. بر اساس مستندات موجود، سه سطح از اختیار برای تیم نسبت به حوزه کاری آن قابل تعریف است:

اختیار کامل: تیم می تواند بدون نیاز به تأییدیه مدیریت جهت انجام عملیات پاسخگویی یا ترمیم، تصمیم گیری نماید.

اختیار اشتراکی: تیم در روال تصمیم گیری جهت پاسخگویی به رویداد امنیتی مشارکت می کند. در واقع تیم می تواند در تصمیم اتخاذ شده تأثیرگذار باشد اما تصمیم گیر نیست.

بدون اختیار: تیم نمی تواند هیچ تصمیمی یا عکس العملی را بدون اجازه انجام دهد. در واقع در این حالت تیم در قالب یک مشاور برای سازمان عمل می کند و پیشنهادات و توصیه های خود را ارائه می کند، اما نمی تواند هیچ اجباری به سازمان وارد نماید.

سرمایه گذاری و هزینه

عدد مشخصی را نمی توان به عنوان هزینه راه اندازی و اداره یک تیم CSIRT ارائه نمود. هزینه راه اندازی یک تیم بستگی به شرایط و محیطی دارد که تیم در آن تأسیس می شود. یک تیم داخلی توزیع شده هزینه ای برای حقوق اضافی یا تجهیزات نیاز ندارد در حالیکه تیم جدیدی که در دپارتمان خود ایجاد می شود هزینه های راه اندازی بالایی را می طلبد. این هزینه شامل هزینه های راه اندازی و هزینه های پرسنلی می باشد. هنگامی که تیم عملیاتی شد، هزینه های نگهداری برای پرسنل (افزایش حقوق یا تعداد پرسنل و آموزش) و همچنین تجهیزات و کار اضافه خواهد شد.

استراتژی های معمول برای تأمین بودجه CSIRT در جدول صفحه بعد گنجانده شده است.

استراتژی های تأمین بودجه		
استراتژی	توصیف	مثال
حق عضویت	حق عضویتی که در بازه های زمانی مشخص برای دریافت طیفی از خدمات پرداخت می شود.	AusCERT حق عضویت دریافت می کند.
خدمات قراردادی	پرداخت برای خدمات در زمان ارائه آنها	CanCERT به ارائه خدمات پولی می پردازد.
حمایت دولتی	یک دپارتمان دولتی برای تیم سرمایه گذاری می کند.	FedCIRC توسط دولت آمریکا حمایت می شود.
حمایت تحقیقاتی یا دانشگاهی	یک دانشگاه یا شبکه تحقیقاتی برای تیم سرمایه گذاری می کند.	CERT-NL توسط شبکه های تحقیقاتی SURFnet حمایت می شود.
سرمایه گذاری سازمان اصلی	یک سازمان تأسیس و سرمایه گذاری تیم را به عهده می گیرد.	تیم های محلی مانند مواردی که در زیمنس یا MCI WorldCom تشکیل شده اند.
حمایت کنسرسیوم	گروهی از دانشگاهها، سازمانها و بخش های دولتی تأمین بودجه را به عهده می گیرند.	
ترکیبی از موارد فوق	مثلاً تأمین بودجه از طریق حمایت دولتی همراه با قراردادهای خصوصی انجام می شود.	CERT/CC توسط دولت و بخش خصوصی تأمین می شود.

سرویس ها

CSIRT سرویس های گوناگونی را می تواند پیشنهاد دهد. برخی از این سرویس ها مستقیماً مربوط به مدیریت رویداد به عنوان هسته سرویس های CSIRT می باشد. سرویس های دیگر مانند آموزش امنیتی یا گزارشات نظارتی که سازمانهای امنیتی به آن نیاز دارند فقط ممکن است به صورت غیرمستقیم مربوط به مدیریت رویداد باشد. بواسطه ماهیت بعضی از این سرویس ها، ممکن است قسمت های دیگر یک سازمان به جای CSIRT درگیر فراهم آوردن آن ها باشند. چینش این مسئولیتها و کارها وابسته است به ساختار سازمان میزبانی که CSIRT در آن قرار دارد.

سرویس های CSIRT را می توان به طور کلی به ۳ دسته تقسیم نمود:

۱. سرویس های واکنشی:

این سرویس ها به وسیله یک رویداد یا یک درخواست، مانند گزارش به خطر افتادن یک میزبان، گسترش کدهای مخرب، آسیب پذیری نرم افزار یا موردی که توسط یک سیستم تشخیص نفوذ یا سیستم ثبت وقایع تشخیص داده شده است، فعال می شوند. سرویس های واکنشی مولفه اصلی کار CSIRT است.

۲. سرویس های بازدارنده:

این سرویس ها اطلاعاتی را فراهم می آورد که کمک به آماده سازی، محافظت و تأمین ایمنی سیستم های حوزه عمل در پیش بینی حملات، مشکلات و رویدادها می نماید. کارایی این سرویس ها مستقیماً تعداد حوادث را در آینده کاهش می دهد.

۳. سرویس های مدیریت کیفی امنیت:

این سرویس ها تقویت کننده سرویس هایی است که در حال حاضر به خوبی بنا شده اند و به صورت سنتی بوسیله قسمت های دیگر سازمان مانند بخش های فناوری اطلاعات، نظارت یا آموزش انجام می شود. این سرویس ها عموماً بازدارنده اند اما غیرمستقیم به کاهش تعداد حوادث کمک می کنند.

انواع سرویس های CSIRT		
سرویس های مدیریت کیفیت امنیت	**سرویس های بازدارنده**	**سرویس های واکنشی**
✓ تحلیل ریسک	✓ اعلان ها	✓ اعلان خطر و هشدارها
✓ طرح ترمیم خرابی و تداوم کار	✓ مشاهده و بررسی تکنولوژی	✓ مدیریت رویداد
✓ مشاوره امنیتی	✓ بررسی و ارزیابی امنیتی	○ تحلیل رویداد
✓ آگاه سازی	✓ پیکر بندی و نگهداری ابزارها، برنامه های کاربردی، زیرساختها و سرویس های امنیتی	○ پاسخگویی به رویداد در محل
✓ آموزش	✓ توسعه ابزارهای امنیتی	○ پشتیبانی پاسخگویی به رویداد
✓ ارزیابی و تأیید محصول	✓ سرویس های تشخیص نفوذ	○ هماهنگی در پاسخگویی به رویداد
	✓ انتشار اطلاعات مربوط به امنیت	✓ مدیریت آسیب پذیری
		○ تحلیل آسیب پذیری
		○ پاسخگویی به آسیب پذیری
		○ هماهنگی در پاسخگویی به آسیب پذیری
		✓ مدیریت آثار باقیمانده از حمله
		○ تحلیل آثارباقیمانده از حمله
		○ پاسخگویی به آثار باقیمانده از حمله
		○ هماهنگی در پاسخگویی به آثارباقیمانده از حمله

کارکنان

شناسایی اعضای تیم مدیریت رویداد بسیار مهم است. ممکن است این کارکنان تمام وقت بوده و تنها به این کار مشغول باشند و یا پاره وقت باشند؛ بطوریکه تنها در زمان وقوع یک رویداد کنار هم قرار گرفته و به رفع مشکل می پردازند.

اندازه تیم و تعداد نفرات

یکی از سوالات مهمی که درباره تیم ها پرسیده می شود بزرگی و اندازه تیم است. پاسخ دادن به این سوال آسان نیست و به عوامل زیادی بستگی دارد. اکثر افرادی که درگیر مدیریت رویداد هستند متفق القول هستند که یک نفر کافی نیست، اما درباره تعداد اعضای تیم استاندارد خاصی وجود ندارد. در واقع تعداد کارکنان به میزان تجربه آنها، حجم و تعداد رویدادها و انواع سرویس های ارائه شده بستگی دارد.همچنین تعداد نفرات مورد نیاز به سرویس های ارائه شده در رابطه با مدیریت رویداد و امنیت کامپیوتر توسط سایر بخش های سازمان نیز بستگی دارد. سطح سرویس ارائه شده نیز حداقلی را برای اندازه تیم مشخص می کند.

جایگاه نفرات

با وجود آنکه درباره تعداد اعضای تیم استانداردی وجود ندارد اما درباره جایگاه نفرات در یک تیم استانداردهای توافق شده ای وجود دارد. در اکثر مستندات ارائه شده که روشهای مختلفی را

برای ساختن و سازماندهی یک تیم بیان می کنند، مستقل از مدل سازمانی اتخاذ شده، برخی نقش ها و جایگاهها به طور ثابت و قطعی معرفی شده اند.

- **مدیر یا هماهنگ کننده:** این نقش مسئولیت مدیریت تیم و سرپرستی فعالیتهای مربوط به مدیریت رویداد را دارد. این فرد می تواند در مواقع نیاز، منابع بیشتری را درخواست و یا اختصاص دهد. وی کنترل بودجه را نیز می تواند در دست داشته باشد و اختیار دارد تا در شرایط خاص و تعریف شده و در محدوده مشخص به عملیات بپردازد.
- **افراد فنی** (مدیر رویداد یا تحلیلگر حفره امنیتی یا آثار باقیمانده از نفوذ): این افراد پشتیبانی اولیه برای مدیریت رویداد و سایر سرویس های ارائه شده را تأمین می کنند. ممکن است آنها اعضای تمام وقت تیم باشند و یا اعضای کمکی که در مواقع نیاز به یاری CSIRT می شتابند.
- **اولین پاسخگویان:** این نقش شامل افرادی است که اولین گزارش یک رویداد را مدیریت می کنند. آنها معمولاً کارکنان بخش کمک رسان هستند.
- **متخصصان:** این نقش می تواند شامل متخصصان امنیت کامپیوتر، متخصصان پایگاه داده یا مدیران شبکه باشند که برای

کمک و راهنمایی حین برخورد با یک رویداد به کار گرفته می شوند؛ اما اعضای تمام وقت تیم نیستند.

- **سایر نیروهای پشتیبانی حرفه ای یا اداری:** نیروهای پشتیبانی حرفه ای می توانند شامل افرادی از دپارتمانهای فناوری اطلاعات، منابع انسانی، حقوقی، امنیت شرکت و سازمان، ترمیم خرابی و روابط عمومی باشند. همچنین باید شامل متخصصان رسانه، متخصصان بررسی جرایم و سایر افرادی باشد که می توانند به CSIRT یاری برسانند. بخش پشتیبانی اداری نیز شامل منشی ها و سایر نیروهای مشابه است که ممکن است تمام وقت یا پاره وقت باشند و در زمان های نیاز به کمک تیم بشتابند.

مهارت های نفرات

برای تأسیس یک CSIRT با قابلیت مدیریت بالا به افرادی با تخصص ها و مهارت های ویژه احتیاج است که توانایی لازم برای پاسخ به رویدادها، انجام تحلیل ها و برقراری ارتباط موثر با حوزه کاری و صلاحیت حل مشکلات را دارا باشند، به راحتی با تغییرات سازگار شوند و در کارهای روزمره خود افراد موثری باشند. گاهی اوقات پیدا کردن چنین افرادی کار راحتی نیست، به همین دلیل در بسیاری از مواقع CSIRT اعضای داخلی خود را برای انجام عمل مدیریت رویدادها آموزش داده و تربیت می کند.

مجموعه مهارت های پایه ای که اعضای یک CSIRT باید داشته باشند در سه گروه مهارتهای فردی، مهارتهای فنی ومهارت های مدیریت رویداد در زیر بیان شده است.

۱. **مهارت های فردی**
   - ارتباطات (ارتباط نوشتاری، ارتباط گفتاری)
   - سیاست
   - توانایی دنبال کردن سیاست ها و روش ها
   - مهارت های گروهی
   - راستی و امانتداری
   - دانستن محدودیت های هر فرد
   - از عهده استرس بر آمدن
   - حل مسأله
   - مدیریت زمان

۲. **مهارت های پایه فنی**
   - اصول امنیتی
   - حفره ها و ضعف های امنیتی
   - اینترنت
   - خطرها
   - پروتکل های شبکه
   - نرم افزارهای کاربردی و سرویس های شبکه

- مباحث امنیت شبکه
- مباحث امنیتی میزبان/سیستم
- کدهای خرابکار (ویروسها،کرمها، تروجانها)
- مهارت های برنامه نویسی

۳. مهارت های مدیریت رویداد

- سیاست ها و روش های محلی گروه
- درک و تشخیص تکنیک های نفوذ
- ارتباط با سایتها
- تحلیل رویدادها
- نگهداری رکوردهای رویدادها

فصل ۵ - CSIRT ملی

از دیدگاه فنی – امنیتی تیم های ملی می توانند:

- به عنوان نقطه ارتباطی مورد اعتماد، خدمت کنند.
- زیرساختی را برای هماهنگی پاسخگویی به رویدادهای امنیتی کامپیوتری در سطح یک کشور ایجاد و توسعه دهند.
- در عملیات کنترل و نظارت بر فضای مجازی شرکت نمایند. (ترویج و ایجاد گروهی از تیم های ملی و منطقه ای که اطلاعات، تحقیقات، استراتژی های پاسخ و پیام های هشدار اخیر را با یکدیگر و با نقاط مشابه ارتباطی از طریق زیرساختهای خود و حتی در آن سوی مرزهای ملی به اشتراک می گذارند.)
- به سازمانها و موسسات درون کشور برای توسعه توانایی مدیریت رویداد کمک کنند. (برای مثال فراهم نمودن راهنما و اطلاعات برای برنامه ریزی و پیاده سازی تیم ها، ایجاد ارتباطات لازم و تشویق برای بحث و گفتگو میان نمایندگی های دولتی، بنگاههای خصوصی/عمومی یا سازمانهای آکادمیک). این کار ممکن است منجر به توسعه خطوط اصلی و روش های محک زنی یا ارزیابی توانایی های این تیم ها گردد.

همچنین ممکن است شامل یک مکانیزم برای تصدیق یا معتبر ساختن سازمانهای CSIRT درون یک کشور باشد.

- لیستی از توانایی های CSIRT و نقاط ارتباطی درون یک کشور را نگهداری کنند.

شکل زیر مجموعه مراحلی را نشان می دهد که لازمه تأسیس یک تیم CSIRT ملی است.

شکل: مراحل سطح بالای ایجاد CSIRT

طی مراحل از آموزش و آگاهی های اولیه تا رسیدن به مرحله همکاری کاری زمانبر است، مخصوصاً که تیم مورد انتظار، تیمی با قابلیت های ملی باشد. با توجه به منابع فراهم شده از ذینفعان و حوزه های عملیاتی، یک CSIRT می تواند ظرف مدت ۱۸ تا ۲۴ ماه به قابلیت های عملیاتی کاملی برسد. این نمودار می تواند بازتر و گسترده تر و یا جمع تر شود که بستگی به عوامل و تصمیمات اتخاذ شده دارد. این امکان وجود دارد که بخش هایی از مراحل پیاده سازی و عملیاتی همپوشانی داشته باشند.

فصل ٦ - بررسی CSIRT در ایران

با ورود اینترنت به ایران در اوائل دهه هفتاد، به تدریج استفاده از این رسانه در سطح کشور رواج پیدا کرد. با گذشت حدود یک دهه از ورود اینترنت و در اوائل دهه هشتاد، با توجه به افزایش نفوذ اینترنت به منازل، شرکتها و ادارات و رشد تعداد کاربران انتهایی و همچنین رشد تعداد حملات و نفوذهای کامپیوتری، امنیت شبکه های اینترنتی و کامپیوتری اهمیت بیشتری پیدا کرد.

در سال ۸۲ دو فعالیت موازی جهت ایجاد IRCERT شکل گرفت. گروهی دانشجویی در دانشکده فنی دانشگاه تهران و با حمایت شورای عالی اطلاع رسانی تشکیل گردید که نتایج کار خود را در سایت ircert.org و با عنوان مرکز فوریت های امنیت رایانه ای مرکز آمار و انفورماتیک دانشگاه تهران منتشر می کرد. گروه دوم شامل گروهی از فارغ التحصیلان رشته مهندسی کامپیوتر دانشگاه صنعتی شریف بود که به مدد تجارب شخصی خود در بحث امنیت و مطالعات انجام شده درباره CERT، در قالب یک شرکت خصوصی اقدام به ایجاد گروه امداد امنیت کامپیوتری ایران نمودند و نتایج کار خود را در سایت ircert.com منتشر می کردند. فعالیت های این دو گروه در حال حاضر به دلیل عدم وجود حمایت های لازم متوقف گردیده است.

مرکز تحقیقات مخابرات ایران نیز از سال ۱۳۸۳ به این موضوع پرداخت و فاز یک از پروژه ایجاد مرکز مقابله و پاسخگویی به حوادث (CERT) و آماده سازی بستر هماهنگی (Coordination) را در سال ۸۵ به پایان برد. پس از آن این مرکز به ایجاد آپا پرداخت. آپا مخفف آگاهی رسانی، پشتیبانی و امداد است که در حوزه امنیت فضای تبادل اطلاعات خدمات مربوطه را ارائه می دهد. بنابر اطلاعات اعلام شده در سایت آپا به نشانی ircert.cc مأموریت این تیم که در پژوهشکده امنیت ارتباطات و فناوری اطلاعات مرکز تحقیقات مخابرات ایران تشکیل شده، بیشتر جنبه پژوهشی–تخصصی در حوزه مدیریت پاسخگویی به حوادث را مد نظر قرار داده و با ایجاد هفت مرکز آپای تخصصی در دانشگاههای کشور، به مسائل فرهنگ سازی و تربیت نیروی انسانی متخصص در حوزه پاسخگویی به حوادث از یک طرف و انتقال دانش و فناوری این حوزه در داخل کشور از سوی دیگر توجه نموده است. هفت مرکز تخصصی ایجاد شده عبارتند از:

- دانشگاه صنعتی شریف با مأموریت تخصصی در حوزه حوادث مرتبط با بانکهای اطلاعاتی
- دانشگاه صنعتی امیرکبیر با مأموریت تخصصی در حوزه حوادث مرتبط با سیستم عامل

- دانشگاه صنعتی اصفهان با مأموریت تخصصی در حوزه حوادث مرتبط با تجهیزات شبکه
- دانشگاه امام حسین با مأموریت تخصصی در حوزه حوادث مرتبط با سیستم های رمز نگاری
- دانشگاه یزد با مأموریت تخصصی در حوزه حوادث مرتبط با نرم افزارهای کاربردی
- دانشگاه تربیت مدرس با مأموریت تخصصی در حوزه حوادث مرتبط با اسپم
- دانشگاه فردوسی مشهد با مأموریت تخصصی در حوزه حوادث مرتبط با سرویس های شبکه