راهنمای سریع CSIRT

فهرست

مفاهیم ۳

تاریخچه ۴

وضعیت فعلی CSIRTها در دنیا ۶

سرویس های CSIRT ۸

راهنمای تشکیل یک CSIRT ۹

راهنمای انتخاب اعضای CERT ۱۰

مروری بر پروسه های مدیریت رویداد ۱۲

اسامی متفاوت با معنای مشابه برایCSIRT ۱۲

آغاز

مفاهیم

- تیم پاسخگویی به رویداد امنیتی کامپیوتر(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 معمولا برای محدوده مشخص تعریف می شود که می تواند یک شرکت، اداره دولتی، سازمان آموزشی یا یک منطقه یا کشور باشد.

- رویداد امنیتی کامپیوتری

عمل نقض یک سیاست امنیتی ضمنی یا صریح

- رسیدگی به رویداد

رسیدگی به رویداد شامل چند بخش است:

۱. شناسایی و گزارش کردن – توانایی و امکان دریافت و مرور اطلاعات وقایع، گزارشهای رویداد و اعلام خطرها
۲. Triage– فعالیتهای لازم برای مرتب سازی، دسته بندی، اولویت بندی و واگذاری وقایع و رویدادها. مثل یک بیمارستان که در آن بیمارانی که نیاز دارند به سرعت مورد معاینه قرار گیرند، از کسانی که می توانند صبر کنند، جدا می شوند و اولویت بندی می گردد.
۳. تحلیل – بررسی و تصمیم گیری درباره آنکه چه اتفاقی افتاده است، به چه تاثیر و خسارتی منتج خواهد شد و گامهای ترمیم یا محدودسازی خطرات چه هستند. این مرحله می تواند شامل مشخص کردن تهدیدات جدیدی که زیرساختها را تحت تاثیر قرار می دهد نیز باشد.
۴. پاسخگویی به رویداد – فعالیتهای لازم جهت حل کردن یا کاهش خسارات یک رویداد، هماهنگی و انتشار اطلاعات و پیاده سازی استراتژی های پیگیری برای جلوگیری از وقوع مجدد رویداد

- مدیریت رویداد

مدیریت رویداد به پاسخگویی به رویداد و فعالیتهای بازدارنده و پیشگیرانه ای که از وقوع رویدادها جلوگیری می کنند، اطلاق می شود.

تاریخچه

- تولد FIRST

در آگوست سال ۱۹۸۹ کارگاهی توسط *CERT/CC* برگزار شد تا علاوه بر بررسی فعالیتهای سال گذشته، به گامهای آتی در هماهنگ کردن ارتباط بین تیمها بپردازد. این نقطه سرآغازی بود بر کفرانسهای سالانه ای که در حال حاضر به عنوان انجمن تیمهای امنیتی و پاسخگویی رویداد یا *FIRST* شناخته می شود.

در نوامبر سال ۱۹۹۰ ، ۱۱ گروه، انجمن تیمهای امنیتی و پاسخگویی رویداد (*FIRST*) را تاسیس نمودند. در آن زمان شبکه اینترنت حدود ۳۴۰ هزار میزبان داشت. نکته جالب حضور یک تیم فرانسوی در بین موسسان امریکایی این انجمن بود.

FIRST ابتدائا یک شبکه از اعضای ثبت شده است که هریک *CSIRT* یا یک تیم امنیتی هستند. اعضا به صورت داوطلبانه با یکدیگر کار می کنند و بر روی جلوگیری از رویداد، اشتراک اطلاعات، اشتراک تحلیل حفره های امنیتی و هماهنگی فعالیتهای پاسخگویی در زمان بروز یک حادثه امنیتی تمرکز می کنند. اطلاعات بیشتر درباره این انجمن را می توان در سایت ان به نشانی *www.first.org* یافت.

- تولد APCERT

اولین *CSIRT* شناخته شده در منطقه آسیا و اقیانوسیه، متعلق به کشور استرالیاست که *AusCERT* نام دارد و در سال ۱۹۹۳ راه اندازی شده است.

بیشتر تیمهای *CSIRT* در این منطقه در سالهای ۹۶ و ۹۷ تشکیل شدند. برخی تیمها فعالیت خود را داوطلبانه آغاز کردند و پس از مدتی با دریافت بودجه دولتی به تیمهای ملی بدل شدند. از جمله نمونه های این تیمها می توان *CERTCCKR* در کشور کره، *JPCERT/CC* در کشور ژاپن و *SingCERT* در کشور سنگاپور اشاره کرد که از اولین تیمها در منطقه آسیا پاسیفیک بودند و همگی به عضویت *FIRST* نیز درآمدند.

تیمهای آسیایی نیز همانند اروپایی ها به دنبال روشی برای ایجاد همکاری بین تیمها و اشتراک داده در این منطقه بودند. در سال ۱۹۹۷ گروه کاری *APSIRC*[۱] نامیده شد، شکل گرفت. تیمهای اصلی در توسعه این گروه کاری، *CERTCC-KR*، *SingCERT* و *JPCERT/CC* بودند. در سال ۲۰۰۳ گروه کاری *APSIRC* به یک گروه جدید مبدل شد و *APCERT* نام گرفت.

[۱] Asia Pacific Security Incident Response Coordination

وضعیت فعلی CSIRTها در دنیا

- سطح اختیار تیمها

بر اساس مستندات موجود، سه سطح از اختیار برای تیم نسبت به حوزه کاری آن قابل تعریف است:

۱. اختیار کامل: تیم می تواند بدون نیاز به تاییدیه مدیریت جهت انجام عملیات پاسخگویی یا ترمیم تصمیم گیری نماید. برای مثال یک تیم با اختیار کامل می تواند طی یک حمله از سوی یک نفوذگر، به مدیر شبکه دستور دهد که یک سیستم را از شبکه قطع نماید.
۲. اختیار اشتراکی: تیم در روال تصمیم گیری جهت پاسخگویی به رویداد امنیتی مشارکت می کند. در واقع تیم می تواند در تصمیم اتخاذ شده تاثیر گذار باشد اما تصمیم گیر نیست.
۳. بدون اختیار: تیم نمی تواند هیچ تصمیمی یا عکس العملی را بدون اجازه انجام دهد. در واقع دراین 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. برای مثال CERT/CC تیمی است که هیچ اختیاری بر روی حوزه عمل خود که اینترنت است، ندارد.

- استراتژی های تامین بودجه
  - حق عضویت: مبلغی که در بازه های زمانی مشخص برای دریافت طیفی از خدمات پرداخت می شود.
  - خدمات قراردادی: پرداخت برای خدمات در زمان ارائه آنها .
  - حمایت دولتی: یک دپارتمان دولتی برای تیم سرمایه گذاری می کند .
  - حمایت تحقیقاتی یا دانشگاهی: یک دانشگاه یا شبکه تحقیقاتی برای تیم سرمایه گذاری می کند .
  - سرمایه گذاری سازمان اصلی: یک سازمان تاسیس و سرمایه گذاری تیم را به عهده می گیرد.

- حمایت کنسرسیوم: گروهی از دانشگاهها، سازمانها و بخشهای دولتی تامین بودجه را به عهده می گیرند.
- ترکیبی از موارد فوق: مثلا تامین بودجه از طریق حمایت دولتی همراه با قراردادهای خصوصی انجام می شود.

جایگاه نفرات در تیمها

- مدیر یا هماهنگ کننده: این نقش مسئولیت مدیریت تیم و سرپرستی فعالیتهای مربوط به رسیدگی به 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 رسیدگی به رویداد وسایر سرویس های ارائه شده را تامین میکنند. 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 معمولا کارکنان بخش کمک رسان هستند.

- متخصصان: این نقش می تواند شامل متخصصان امنیت کامپیوتر، متخصصان پایگاه داده یا مدیران شبکه باشد که برای کمک و راهنمایی حین برخورد با یک رویداد افزوده میشوند اما اعضای تمام وقت تیم نیستند.

- سایر نیروهای پشتیبانی حرفه ای یا اداری: نیروهای پشتیبانی حرفه ای میتوانند شامل افرادی از دپارتمانهای فناوری اطلاعات، منابع انسانی، حقوقی، امنیت شرکت و سازمان، ترمیم خرابی و روابط عمومی باشد. همچنین باید شامل متخصصان رسانه، متخصصان بررسی جرایم وسایر افرادی باشد که می توانند به CSIRT یاری رسانند. 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.

سرویس های CSIRT

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

۱. سرویس های واکنشی

این سرویس ها بوسیله 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 پیشگیرانه

این سرویس ها اطلاعاتی را فراهم می آورد که کمک به آماده سازی، محافظت و تامین ایمنی سیستمهای حوزه عمل در پیش بینی حملات، مشکلات و رویدادها و پیشگیری از آنها 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 درحال حاضر به خوبی بنا شده و

- مستقل از مدیریت رویداد هستند.
- به صورت سنتی بوسیله قسمت های دیگر سازمان مانند بخش های فناوری اطلاعات، نظارت یا آموزش انجام می شود.

راهنمای تشکیل یک CSIRT

- مراحل سطح بالای ایجاد یک CSIRT

مرحله اول- آموزش ذی نفعان درباره توسعه تیمی در سطح ملی.

مرحله دوم – برنامه ریزی برای ایجاد *CSIRT*

مرحله ۳ – پیاده سازی *CSIRT*

مرحله ۴- عملیاتی کردن *CSIRT*

مرحله پنجم – همکاری

- لیست عملیاتی ایجاد یک CSIRT

۱. واسطها و تعاملات تعریف شوند
۲. تعریف نقشها، مسئولیتها و اختیارات متناظر
۳. مستندسازی گردش کار
۴. تولید سیاستها و روالهای مربوطه
۵. یک برنامه پیاده سازی ایجاد کنید و درخواست بازخورد نمایید.
۶. هنگامی که تیم عملیاتی شد، CSIRT را رسما معرفی نمایید.
۷. تعریف روشهایی برای ارزیابی کارایی تیم
۸. یک برنامه پشتیبان برای هر المان تیم داشته باشید.
۹. منعطف باشید .
۱۰. شناسایی دینفعان و مشارکت کنندگان
۱۱. به دست آوردن حمایت و پشتیبانی مدیریت
۱۲. ایجاد یک طرح پروژه برای CSIRT

۱۳. جمع آوری اطلاعات
۱۴. شناسایی حوزه عملیاتی CSIRT
۱۵. تعریف ماموریت CSIRT
۱۶. بودجه برای عملیات تیم
۱۷. تصمیم گیری درباره طیف و سطح سرویسهایی که تیم ارائه خواهد کرد.
۱۸. تصمیم گیری درباره ساختار گزارش دهی، اختیارات و مدل سازمانی تیم
۱۹. شناسایی منابع لازم مانند کارمندان، تجهیزات و زیرساخت

راهنمای انتخاب اعضای CERT

ترکیب اعضای *CSIRT* در گروههای مختلف متفاوت است و به پارامترهای مختلفی بستگی دارد؛ ازجمله:

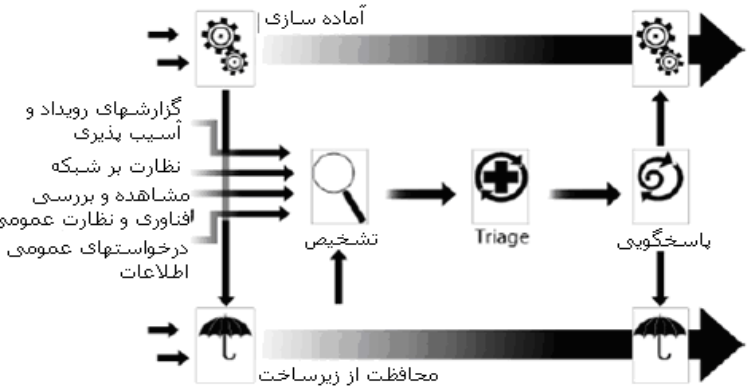
- اهداف آن تیم
- طیف سرویسهای ارائه شده
- متخصصین در دسترس و موجود
- اندازه حوزه کاری و تکنولوژی پایه آن
- بار و حجم رویدادهای پیش بینی شده
- پیچیدگی گزارشهای رویدادها
- بودجه

- مهارتهای فردی
  - ارتباطات
    - ارتباط نوشتاری
    - ارتباط گفتاری
  - مهارتهای ارائه
  - سیاست
  - توانایی دنبال کردن سیاستها و روشها
  - مهارتهای گروهی
  - راستی و امانتداری

- دانستن محدودیتهای هر فرد
- از عهده استرس برآمدن
- حل مسأله
- مدیریت زمان

- مهارتهای پایه فنی
  - اصول امنیتی
  - حفره‌ها و ضعفهای امنیتی
  - اینترنت
  - خطرها
  - پروتکلهای شبکه
  - نرم‌افزارهای کاربردی و سرویسهای شبکه
  - مباحث امنیت شبکه
  - مباحث امنیتی میزبان/سیستم
  - کدهای خرابکار (ویروسها، کرمها، تروجانها)
  - مهارتهای برنامه نویسی
- مهارتهای رسیدگی به رویداد
  - سیاستها و روشهای محلی گروه
  - درک و تشخیص تکنیکهای نفوذ
  - ارتباط با سایتها
  - تحلیل رویدادها
  - نگهداری رکوردهای رویدادها

مروری بر پروسه های مدیریت رویداد



اسامی متفاوت با معنای مشابه برایCSIRT

تیم پاسخگویی به رویداد امنیتی کامپیوتری	CSIRT
توانایی پاسخگویی به رویداد امنیتی کامپیوتری	CSIRC
توانایی پاسخگویی به رویداد کامپیوتری	CIRC
تیم پاسخگویی به رویداد کامپیوتری	CIRT
تیم مدیریت رویداد	IHT
مرکز پاسخگویی به رویداد یا توانایی پاسخگویی به رویداد	IRC
تیم پاسخگویی به رویداد	IRT
تیم پاسخگویی به فوریت های امنیتی	SERT
تیم پاسخگویی به فوریت های کامپیوتری	CERT
تیم پاسخگویی به رویداد امنیتی	SIRT