CERT & CSIRT

ایجاد مراکز ماهر و گوهر

مرکز امداد و هماهنگی رایانه – گروه های واکنش هماهنگی رخداد

(Computer Security Incident Response Team**)**

امروزه معلومات و اطلاعات به عنوان دارایی محسوب می شود و محافظت از دارایی ها یک اصل است . حادثـه روز سوم نوامبر سال ۱۹۸۸ که در آن ویروس کـامپیوتری مـوریس ورم (morris worm) درصـد زیـادی از کامپیوترها را در آن زمان گرفتار کرد در واقع نمونه یک تهدید عملی یا حمله بود. ایـن رویـداد بعنـوان سـابقه برجای ماند و متخصصین را مجبور به یافتن راه چاره ای برای اینگونه حوادث رایانه ای نمود. در آن سال تیمـی تحت عنوان گروه پاسخگویی به رخدادها (CSIRT) در دانشگاه کارنگی ملون آمریکا تشکیل و آغاز بکار کرد.

CSIRT ها گروههایی هستند که هدف اصلی آنها پاسخگویی مناسب به رویدادهای امنیتی کامپیوتری می باشد و ذیل هدف می تواند آموزش به افراد در محافظت از سیستم هـای خـود در دنیـای ارتباطـات باشـد. بـدنبال شناخت و توسعه این گروهها (CSIRT) نیاز به هماهنگی و برنامه ریزی درون و برون سـازمانی ضـرورت پیـدا کرد و مراکزی تحت نام (CERT) بنیان گذاشته شد.

در کشور ما و دیگر همسایگان در منطقه جهت پیـاده سـازی مـوارد ذکـر شـده و ایجـاد زیرسـاختهای امنیتـی کامپیوتری راه کارهایی مطرح که در ذیل بیان می شود:

۱. رویکرد از پائین به بالا (اول ایجاد گروههای CSIRT دوم ایجاد مراکز CERT)

۲. رویکرد بالا به پائین (اول ایجاد مراکز CERT بعد ایجاد گروه های CSIRT)

با برپایی اولین همایش تخصصی امداد و هماهنگی رویـدادهای کـامپیوتری در اسـفندماه ۱۳۸۷- ترکیبـی از دو رویکرد یادشده جهت پیاده سازی و اجرا در وزارت ارتباطات و فناوری اطلاعات پیش روی قرار گرفت.

لازم بذکر است باتوجه به نظرات کارشناسان و مدیران وزارت ارتباطات و فناوری اطلاعات، CSIRT یـا گـروه های پاسخگو به رویدادهای کامپیوتری اختصاراً گوهر (گروه های واکنش هماهنگی رخداد) نامیـده مـی شـوند و مراکز امداد و هماهنگی کامپیوتری (CERT) نیز اختصاراً ماهر (مرکز امداد و هماهنگی رایانـه ای) نامیـده مـی شوند. نظر به موارد یاد شده انگیزه های تاسیس گروه های پاسخگو به رویدادهای امنیتی کـامپیوتری مـی توانـد شامل موارد ذیل باشد:

۱. افزایش تعداد گزارشات دریافتی از رویدادهای امنیتی کامپیوتر
۲. اتخاذ استراتژی مدیریت بحران
۳. تدوین قوانین و مقررات جدید برای محافظت از دارایی ها (اطلاعات)
۴. مدیران شبکه و سیستمها به تنهایی نمی توانند از دارایی و سیستم های سازمان محافظت کنند
۵. طراحی و استراتژی در این امر مهم است.

*** مزایای مراکز امداد و هماهنگی رایانه ای** CERT

۱. هماهنگی مرکزی برای رویدادهای امنیتی کامپیوتر
۲. ارائه پاسخ سیستماتیک جهت رویدادهای امنیتی
۳. توانایی احیاء سریع و کارآمد سیستم ها و شبکه
۴. تعامل فراگیر با مباحث قانونی و بودجه

*** مراحل تشکیل و تنظیم گوهرها یا (**CSIRT**) و شرح عناصر آن:**

۱. موسسین و گردانندگان آن

۲. تعیین اهداف ، چشم انداز و ارزشها

۳. تعیین روابط و ملاحظات سازمانی

۴. معرفی و تعریف سرویس ها

۵. بودجه و سرمایه گذاری

۶. ارائه تسهیلات و امکانات

۷. تعیین خط مشی و سیاست ها

شرح عناصر تشکیل دهنده :

*** موسسین CERT و CSIRT شامل :**

۱. بخش آکادمیک = تمرکز روی R&D ، سرویس دهی کاربران با موسسات آکادمیک

۲. بخش های بحرانی = بخش کنترل شده بالای سازمانی – بخش اضطراری – سرویس دهنده سازمانی

۳. CERTهای ملی (کشوری)= سرویس دهی همه کاربران اینترنت در کشور

۴. CSIRT های تجاری = سرویس دهی به پرداخت مشتریان

۵. CSIRT های فروشنده = پشتیبانی محصولات و فروشندگان

*** اهداف ، چشم اندازها و ارزشها در CERT**

۱. تعیین اهداف گروه و چشم انداز آن } برقراری اهداف
} توجه مستمر به فعالیت ها و هدف اصلی

۲. شناسایی ارزشهای گروه } انتصاب ارزشها به اعضاء گروه

❋ ملاحظات سازمانی برای ایجاد CERT

۱. بررسی مجوزها یا عدم صدور مجوز برای گروه های CSIRT

۲. سلسله مراتب سازمانی { تعیین چارت سازمانی گروه های CSIRT
تعیین افراد جهت دریافت گزارشات CSIRT

۳.تعاملات سازمانی CSIRT { تعیین محدوده فعالیت سازمانی
تعیین کار در بخش های خارجی سازمان

۴.اختصاص تشویقات در جهت اهمیت دادن به توسعه دانش و اطلاعات مربوط بـه رویـداد امنیتـی – تحلیلگـر ویروس – تحلیلگر تهاجم – تحلیلگر امنیت شبکه و متخصص برنامه های کاربردی تحت وب

❋ سرویس های گروه های CSIRT

۱. سرویس های پشتیبانی (فعال)

۲. سرویس های مرکزی واکنشی (عکس العمل)

۳. سایر سرویس ها (همچون سرویس مدیریت امنیت اطلاعات)

❋ سرمایه گذاری برای CERT

- استراتژی تامین اعتبار مالی گروه های CSIRT

۱. تحت پوشش سرمایه گذاری دولتی

۲. راهبردهای اعضاء

۳. استفاده از سرویس های درآمدزا

۴. استفاده از سرویس های تحت قرارداد

۵. تامین اعتبار مراکز تحقیقاتی و دانشگاهی

۶. سرمایه گذاری در سازمان های مولد

۷. سرمایه گذاری بصورت کنسرسیوم (قرارداد اقتصادی تجاری چند شرکت)

*** تسهیلات مراکز ماهر و گوهر**

- فراهم نمودن اتصالات شبکه ایمن برای دسترسی

- فراهم نمودن سیستم مدیریت مربوط به مشتریان یا معادل آن برای پیگیری گزارشات و اتصال با بانک اطلاعاتی

*** تسهیلات طرح ارتباطی (امکانات ارتباطی)**

- تجهیزات ارتباطی (مثل موبایل – تلفن – فکس و غیره)

- کانال های ارتباطی ایمن
  - رمزنگاری email ها برای محرمانگی بیشتر
  - ایمنی وب و تعیین هویت
  - استفاده از اعضاء جهت خاتمه پیام
- سرویس و تائید تماس گیرنده از مخاطب

*** خط مشی و رویه کاری جهت** CERT

۱. تعیین خط مشی (امنیت اطلاعات – امنیت شبکه – امنیت برنامه های کاربردی – امنیت پرسنل)

۲. وضع قوانین (کدهای حرفه ای مورد مصرف – توافق منع افشای اطلاعات- توافق سطوح سرویس)

۳. تعیین روال و رویه کاری

❋ پیاده سازی : CSIRT

- در این مرحله گروه های پاسخگویی به رویدادهای کامپیوتری از اطلاعات بدست آمده از فعالیت های قبلی برای ایجاد CSIRT استفاده می کند.

❋ مدل سازمانی CSIRT**:**

- CSIRT توزیع شده داخی ، CSIRT متمرکز داخلی ، CSIRT متمرکز و توزیع شده داخلی و CSIRT هماهنگ

- گروه های پاسخگو به رویداد امنیتی با پرسنل موجود علاوه بر کار معمول خود ، کار ناظرین شبکه و سیستم های امنیتی را نیز بعنوان بخشی از مسئولیت و وظیفه خود انجام می دهد.

- CSIRT توزیع شده داخلی : سازمان مربوطه ، کارکنان موجود را برای CSIRT توزیع شده بکار می گیرد و رسماً برای انجام فعالیت های پاسخ به رویداد اختصاص می دهد و مدیریتی جهت نظارت بکار آنها وجود دارد. این وظایف علاوه بر کار معمول آنها می باشد و بشکل تمام وقت در نظر گرفته می شود. (حالت کمیته های تخصصی اجرایی)

- CSIRT متمرکز داخلی : این مدل مبتنی بر کارمند است. در بسیاری موارد اعضاء تیم ۱۰۰٪ از وقت کاری خود را برای CSIRT صرف می کنند. (مثل واحدهای سازمانی)

البته این مدل با کارکنان نیمه وقت و چرخشی نیز قابل اجراست.

در هر حال تیم بطور متمرکز در سازمان مستقر است و برای تمام فعالیت ها پاسخ گویی می کند.

- CSIRT متمرکز و توزیع داخلی : ترکیبی از CSIRT توزیع شده و متمرکز را بیان می کند و حداکثر بهره وری کارکنان موجود را در موقعیت های راهبردی در کل سازمان نشان می دهد.

- CSIRT هماهنگ کننده : امور CSIRT سازمان را با سامانهای داخلی و خارجی دیگر هماهنگ می سازد.

این نوع CSIRT به سازمان های دیگر در مباحث مقابله با رویداد کمک می کند و توصیه ، هشدار و یا راه حلی را پیشنهاد یا توزیع می کند.

- آسیب پذیری ها : ضعف ها اغلب ناشی از فقدان مکانیزم دفاع مناسب است و آسیب پذیری ها می توانند ، حملات سایبری را آغاز نماید. (اگر یک تهدید واقعیت یابد، حمله صورت گرفته است)
- حادثه، وقوع یک رویداد ناسازگار مثل مسدودکردن سرویس توسط مهاجم، خرابی توسط ویروس است.
- رسیدگی به رویداد شامل حمایت و بازیابی از شرایط کامپیوتر و اطلاعات ذخیره شده آنان است.

❋ مهارت های کارکنان CSIRT**:**

- مهارت های کارکنان CSIRT شامل مهارتهای شخصی و فنی می شوند که مهارتهای شخصی شامل مهارتهای ارتباطی (شفاهی و نوشتاری) دیپلماسی ، توانایی کار بعنوان عضو یک گروه و همکاری ، توانایی شناخت محدودیت های افراد ، توانایی غلبه بر استرس ، قابلیت حل مسئله ، مدیریت زمان ، توجه به جزئیات و امانت داری و درستی می باشد.

- مهارتهای فنی شامل آگاهی به اصول امنیتی (تعیین هویت – جامعیت – محرمانگی – اعتبارسنجی – عدم انکار – کنترل دسترسی)

- آسیب پذیری ها و نقاط ضعف امنیتی : شامل امنیت فیزیکی – نقاط ضعف پیکربندی – سهل انگاری کاربر و کدهای مخرب مثل ویروس – کرم و تروجان ها همچنین برنامه نویسی ها و تحلیل سیستم

❋ نقش ها و مسئولیت های تیم CERT**:**

شامل مدیر یا سرپرست تیم ، ناظرین و کارکنان خط اول Help Desk ها می باشد.

سپس رسیدگی کنندگان به رویدادها و آسیب ها ، ناظرین شبکه و سیستم و توسعه دهندگان وب ، کارکنان پشتیبانی که هدایت تیم را عهده دار است.

*** سرویس های CSIRT به سه گروه تقسیم می شوند:**

۱. سرویس پیشگیرانه : این سرویس ها اطلاعات و تسهیلات لازم را برای حمایت و امن کردن سیستم ها انجام داده و پیش بینی لازم برای حمله و یا رویدادهای امنیتی را در نظر می گیرد که نتیجه آن کاهش رویدادها در آینده می باشد.

۲. سرویس های واکنشی : با یک رویداد مثل برنامه مخرب و مزاحم فعال می شود و در بخش مرکزی CSIRT حضور دارد تا رفع مشکل صورت گیرد.

۳. سرویس های مدیریت کیفیت امنیت: این سرویس ها ، سرویس های موجود را توسط بخش IT ، ممیزی و آموزش تقویت می کند و در واقع به نحوه پیش فعال در کاهش تعداد رویدادها موثر است.

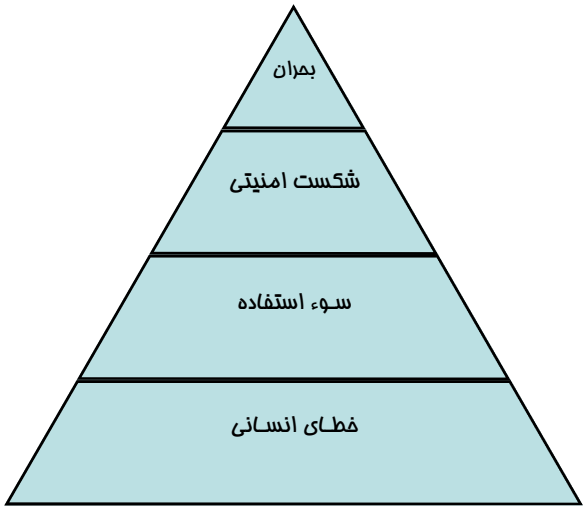
سرویس های واکنشی شامل هشدارها – اخطارها – رسیدگی به رویدادها (تحلیل رویداد ، پاسخ ، پشتیبانی هماهنگی) رسیدگی و ترمیم آسیب های وارده (تحلیل آسیب پذیری – پاسخ – همکاری در پاسخ) می باشد.

- چارچوب CSIRT شامل :

(ماموریت و اهداف – موسسان – جایگاه سازمانی و روابطه آن با سایر سازمانهای مشابه)

دسته بندی رویدادها در CERT

در شکل زیر ۴ سطح جهت رویدادها در نظر گرفته شده است.



سطح اول رویدادها، از افشای اطلاعات و خطاهای انسانی منشاء می گیرد.

سطح دوم رویدادها از سوء استفاده ها نشأت گرفته می شود. (سوء استفاده از email ، استراق سمع الکترونیکی ،

ایجاد محتویات غیرقانونی در نامه ها و غیره است)

سطح سوم از بین رفتن امنیت اطلاعات یا سیستم را شامل می شود.

و سطح آخر ایجاد بحران و یک حادثه است که شامل از کار افتادن سرویس می شود.

من ا... التوفیق

علی ثاقب موفق – فوق لیسانس فناوری اطلاعات